# Comprehensive AWS VPC & Networking Multiple Choice Questions

Generated on: 2025-11-16

## VPC (Virtual Private Cloud)

**1. What is the primary purpose of an Amazon VPC?**

A. To provide a physically isolated network in the AWS cloud.

B. To provision a logically isolated section of the AWS Cloud where you can launch AWS resources.

C. To automatically scale EC2 instances based on demand.

D. To store and retrieve any amount of data from anywhere on the web.

**2. What is the smallest CIDR block you can assign to a VPC?**

A. /8

B. /16

C. /28

D. /24

**3. What is the largest CIDR block you can assign to a VPC?**

A. /16

B. /8

C. /28

D. /10

**4. When you create a new VPC, which of the following components are created by default?**

A. A main route table, a default security group, and a default network ACL.

B. An internet gateway, a NAT gateway, and a public subnet.

C. A default subnet in each Availability Zone.

D. A VPC peering connection and a VPN gateway.

**5. Which of the following is a valid CIDR block for a VPC?**

A. 10.0.0.0/15

B. 172.16.0.0/16

C. 192.168.0.0/29

D. 203.0.113.0/24

**6. What does the "tenancy" attribute of a VPC define?**

A. Whether the VPC is public or private.

B. The AWS region in which the VPC is created.

C. Whether EC2 instances launched in the VPC run on shared or dedicated hardware.

D. The number of subnets that can be created within the VPC.

**7. A VPC spans across which of the following AWS infrastructure components?**

A. A single Availability Zone.

B. All Availability Zones within a Region.

C. Multiple AWS Regions.

D. A single Edge Location.

**8. What is the purpose of VPC Flow Logs?**

A. To provide a real-time stream of all DNS queries made from within the VPC.

B. To capture information about the IP traffic going to and from network interfaces in your VPC.

C. To log all API calls made to the VPC service.

D. To automatically block malicious IP addresses detected within the VPC.

**9. Where can VPC Flow Logs publish their data?**

A. Amazon S3 and Amazon CloudWatch Logs.

B. Amazon DynamoDB and Amazon SQS.

C. AWS Lambda and Amazon SNS.

D. Amazon EC2 instance store and Amazon EBS.

**10. What is a VPC Peering connection?**

A. A connection that allows you to connect your on-premises data center to your VPC.

B. A networking connection between two VPCs that enables you to route traffic between them using private IPv4 or IPv6 addresses.

C. A dedicated physical connection from your premises to AWS.

D. A gateway that allows resources in your VPC to access the internet.

**11. Which of the following statements about VPC Peering is TRUE?**

A. VPC Peering connections are transitive. If VPC A is peered with VPC B, and VPC B is peered with VPC C, then VPC A can communicate with VPC C.

B. VPC Peering connections can be established between VPCs in different AWS accounts and different regions.

C. VPC Peering connections support overlapping CIDR blocks.

D. Security groups can be referenced across a VPC peering connection only if they are in the same region.

**12. What is a key limitation of VPC Peering that a Transit Gateway can solve?**

A. VPC Peering does not support inter-region connections.

B. VPC Peering requires a full mesh of connections for multiple VPCs, which becomes complex to manage.

C. VPC Peering cannot handle traffic from on-premises networks.

D. VPC Peering does not support IPv6 traffic.

**13. What are the two types of VPC Endpoints?**

A. Public and Private Endpoints.

B. Gateway and Interface Endpoints.

C. Regional and Zonal Endpoints.

D. Standard and Express Endpoints.

**14. A Gateway VPC Endpoint provides private access to which AWS services?**

A. Amazon S3 and DynamoDB.

B. Amazon EC2 and RDS.

C. AWS Lambda and API Gateway.

D. Amazon Kinesis and SQS.

**15. How does an Interface VPC Endpoint (powered by AWS PrivateLink) work?**

A. It creates a gateway in your route table to access AWS services.

B. It creates an Elastic Network Interface (ENI) in your subnet with a private IP address that serves as an entry point for traffic destined to the service.

C. It uses an Internet Gateway to route traffic to AWS services over a private channel.

D. It requires a VPN connection to establish a secure link to the service.

**16. You have created a VPC with CIDR 10.0.0.0/16. Can you add a secondary CIDR block of 192.168.0.0/24 to this VPC?**

A. No, secondary CIDR blocks must be from the same RFC 1918 range as the primary.

B. Yes, you can add up to four secondary IPv4 CIDR blocks to a VPC.

C. No, a VPC can only have one CIDR block.

D. Yes, but only if the VPC has dedicated tenancy.

**17. What is the "local" route in a VPC route table?**

A. A route that directs traffic to the internet gateway.

B. A default route that allows communication between instances within the same VPC.

C. A route that points to a virtual private gateway.

D. A route that must be manually added to allow subnet-to-subnet communication.

**18. Can you delete the default VPC created in your AWS account?**

A. No, the default VPC cannot be deleted.

B. Yes, you can delete the default VPC. If you do, you can request AWS support to restore it.

C. Yes, you can delete the default VPC, and you can create a new default VPC yourself via the AWS console or CLI.

D. No, but you can modify its CIDR block.

**19. What is a primary benefit of using a custom VPC over the default VPC?**

A. Higher network performance.

B. Lower data transfer costs.

C. Full control over the network environment, including IP address range, subnets, and route tables.

D. Automatic deployment of resources into public subnets.

**20. VPC Flow Logs do NOT capture which of the following traffic types?**

A. Traffic generated by instances when they contact the Amazon DNS server.

B. Traffic to and from 169.254.169.254 for instance metadata.

C. DHCP traffic.

D. All of the above.

**21. What is the purpose of the DNS resolution setting in a VPC?**

A. It determines if the Amazon-provided DNS server can resolve public DNS hostnames.

B. It controls whether your instances receive public IP addresses.

C. It enables or disables VPC Flow Logs.

D. It defines the domain name for the DHCP options set.

**22. What does enabling "DNS hostnames" for a VPC do?**

A. It allows instances in the VPC to resolve public DNS names.

B. It ensures that instances with public IP addresses get a corresponding public DNS hostname.

C. It assigns a custom domain name to your VPC.

D. It configures the VPC to use a custom DNS server.

**23. You are designing a multi-tier application. Where should you place your database servers for the highest security?**

A. In a public subnet with a restrictive security group.

B. In a private subnet with no route to an Internet Gateway.

C. In a public subnet with a Network ACL blocking all inbound traffic.

D. Directly on an EC2 instance with an Elastic IP address.

**24. If you have two VPCs (VPC-A and VPC-B) with overlapping CIDR blocks, can you establish a VPC peering connection between them?**

A. Yes, but routing will be unpredictable.

B. Yes, but only if they are in different regions.

C. No, VPC peering requires non-overlapping CIDR blocks.

D. Yes, but you must use a NAT Gateway to translate addresses.

**25. What is the maximum number of VPCs you can have per region in an AWS account by default?**

A. 1

B. 5

C. 20

D. 100

**26. Which service acts as a network hub to simplify connectivity between multiple VPCs and on-premises networks?**

A. VPC Peering

B. Internet Gateway

C. AWS Transit Gateway

D. Virtual Private Gateway

**27. When using a Gateway VPC Endpoint for S3, where do you add the route to the endpoint?**

A. In the Security Group of the instance.

B. In the Network ACL of the subnet.

C. In the Route Table associated with the subnets that need access.

D. In the DHCP Options Set for the VPC.

**28. An Interface Endpoint is represented by what component within your VPC?**

A. A route target.

B. A prefix list ID.

C. An Elastic Network Interface (ENI).

D. A virtual gateway.

**29. What is the main advantage of using an Interface Endpoint over a Gateway Endpoint?**

A. Interface Endpoints are free of charge.

B. Interface Endpoints can be accessed from on-premises networks connected via Direct Connect or VPN.

C. Interface Endpoints support more services, specifically S3 and DynamoDB.

D. Interface Endpoints do not require any changes to route tables.

**30. You have a default VPC and you launch an EC2 instance into its default subnet without specifying any network settings. What will be true about this instance?**

A. It will be in a private subnet and cannot access the internet.

B. It will be assigned a private IP address only.

C. It will be assigned both a private IP address and a public IP address.

D. It will fail to launch because a security group was not specified.

**31. What is the scope of a VPC?**

A. Global

B. Availability Zone

C. Region

D. Edge Location

**32. To allow instances in a VPC to resolve DNS hostnames to private IP addresses when queried from another VPC in a peering relationship, what must be enabled?**

A. VPC Flow Logs

B. DNS resolution for the peering connection.

C. Dedicated tenancy for both VPCs.

D. A NAT Gateway in each VPC.

**33. Which of the following IP address ranges is NOT a private, non-routable range according to RFC 1918?**

A. 10.0.0.0/8

B. 172.16.0.0/12

C. 192.168.0.0/16

D. 169.254.0.0/16

**34. When you create a VPC, you must specify a range of IPv4 addresses in the form of a CIDR block. This is the _____ CIDR block for your VPC.**

A. Primary

B. Secondary

C. Public

D. Default

**35. If you want to connect your VPC to your corporate datacenter, which two services could you use?**

A. Internet Gateway and NAT Gateway

B. AWS Direct Connect and AWS Site-to-Site VPN

C. VPC Peering and VPC Endpoints

D. Elastic IP and Security Groups

**36. What is the purpose of a Virtual Private Gateway (VGW)?**

A. To allow internet access for a VPC.

B. To enable communication between two VPCs.

C. To serve as the anchor on the AWS side of a VPN connection or Direct Connect.

D. To provide private access to AWS services like S3.

**37. Can a single VPC have both an Internet Gateway and a Virtual Private Gateway attached?**

A. No, a VPC can only have one type of gateway.

B. Yes, this is a common configuration for a VPC that needs both internet access and a connection to an on-premises network.

C. Yes, but they must be attached to different subnets.

D. No, a Virtual Private Gateway replaces the need for an Internet Gateway.

**38. What is the "Bring Your Own IP" (BYOIP) feature in VPC?**

A. It allows you to use your private IP addresses from your on-premises network inside your VPC.

B. It allows you to bring your publicly routable IPv4 address range from your on-premises network to AWS.

C. It allows you to assign any public IP address you want to your EC2 instances.

D. It is a feature for purchasing IP addresses directly from AWS.

**39. You have enabled VPC Flow Logs. What level of detail can you capture?**

A. Only accepted traffic.

B. Only rejected traffic.

C. Both accepted and rejected traffic.

D. Only traffic to and from the internet.

**40. What is the main difference between a default VPC and a custom VPC regarding subnets?**

A. Default VPCs have only private subnets; custom VPCs can have public and private.

B. Default VPCs have default subnets created in each AZ, which are all public by default. In a custom VPC, you define your own subnets.

C. Custom VPCs cannot have public subnets.

D. Default VPCs have a /24 CIDR block for each subnet; custom VPCs can have any size.

**41. Which component is essential for enabling IPv6 communication for a VPC?**

A. An IPv6-enabled NAT Gateway.

B. Associating an IPv6 CIDR block with the VPC and its subnets.

C. A special IPv6 Internet Gateway.

D. An IPv6-only security group.

**42. What is an Egress-Only Internet Gateway used for?**

A. To allow outbound-only internet communication over IPv4 from instances in a private subnet.

B. To allow outbound-only internet communication over IPv6 from instances in a VPC, while preventing inbound IPv6 connections from the internet.

C. To filter all outbound traffic from a VPC for security inspection.

D. To provide a highly available internet connection for a VPC.

**43. If you delete a VPC, what happens to the resources running within it, such as EC2 instances?**

A. The resources are moved to the default VPC.

B. The resources are stopped but not terminated.

C. You must terminate all instances and other resources in the VPC before you can delete the VPC.

D. The resources are automatically terminated.

**44. A company wants to ensure that all traffic between their VPC and Amazon S3 does not traverse the public internet. What should they use?**

A. A NAT Gateway.

B. A VPC Gateway Endpoint for S3.

C. An Internet Gateway with specific route table rules.

D. A VPC Peering connection to the S3 service.

**45. What is the purpose of a prefix list in the context of VPC?**

A. A list of CIDR blocks for AWS services that can be used as a target in a route table for a gateway endpoint.

B. A list of allowed IP addresses in a security group.

C. A list of denied IP addresses in a network ACL.

D. A list of domain names in a DHCP options set.

**46. You are setting up a VPC and need to ensure that instances can resolve each other's hostnames within the VPC. Which two VPC settings must be enabled?**

A. Enable DNS resolution and Enable DNS hostnames.

B. Enable ClassicLink and Enable DNS support.

C. Enable Network Address Usage metrics and Enable DNS hostnames.

D. Enable DNS resolution and assign a DHCP options set.

**47. What is the maximum number of secondary IPv4 CIDR blocks you can associate with a VPC?**

A. 1

B. 2

C. 4

D. 10

**48. Which of the following is a characteristic of a VPC with 'dedicated' tenancy?**

A. All EC2 instances launched into the VPC will run on hardware that's dedicated to a single AWS account.

B. The VPC has a dedicated, physical connection to the internet.

C. The VPC is guaranteed to have lower latency than a default tenancy VPC.

D. Data transfer costs within the VPC are waived.

**49. Can you change the primary CIDR block of a VPC after it has been created?**

A. Yes, at any time through the VPC console.

B. Yes, but only if there are no resources launched in the VPC.

C. No, the primary CIDR block cannot be changed after creation.

D. No, but you can add a new primary CIDR and deprecate the old one.

**50. VPC sharing allows multiple AWS accounts within an AWS Organization to do what?**

A. Share a single Internet Gateway.

B. Create and manage resources like EC2 instances and RDS databases in shared, centrally managed VPCs.

C. Share S3 buckets without using bucket policies.

D. Share Elastic IP addresses across accounts.

## Subnets

**51. A subnet is a range of IP addresses in your VPC. A subnet must reside entirely within which of the following?**

A. An AWS Region

B. A single Availability Zone

C. An Edge Location

D. A Local Zone

**52. What defines a subnet as a "public subnet"?**

A. The subnet's CIDR block is from a public IP range.

B. The subnet's associated route table has a route to an Internet Gateway.

C. The subnet has the "Auto-assign public IPv4 address" setting enabled.

D. The subnet is part of the default VPC.

**53. What defines a subnet as a "private subnet"?**

A. It is located in a specific, physically secure Availability Zone.

B. Its associated route table does not have a route to an Internet Gateway.

C. It only allows instances with private IP addresses to be launched.

D. Its CIDR block is within the 10.0.0.0/8 range.

**54. In a subnet with CIDR block 10.0.1.0/24, how many IP addresses does AWS reserve?**

A. 2

B. 3

C. 4

D. 5

**55. In a subnet with CIDR block 10.0.1.0/24, which of the following IP addresses is NOT reserved by AWS?**

A. 10.0.1.0

B. 10.0.1.1

C. 10.0.1.4

D. 10.0.1.255

**56. What is the purpose of the IP address ending in .1 (e.g., 10.0.1.1) that AWS reserves in every subnet?**

A. Reserved for the VPC router.

B. Reserved for the Amazon-provided DNS server.

C. Reserved for future use.

D. Reserved as the network broadcast address.

**57. You create a VPC with CIDR 10.0.0.0/16 and a subnet with CIDR 10.0.0.0/24. How many available IP addresses are there for your resources in this subnet?**

A. 256

B. 255

C. 254

D. 251

**58. Can a subnet's CIDR block be modified after it is created?**

A. Yes, it can be resized at any time.

B. No, a subnet's CIDR block cannot be changed. You must create a new subnet and migrate resources.

C. Yes, but only to make it smaller.

D. Yes, but only if there are no instances running in it.

**59. What happens if you enable the "Auto-assign public IPv4 address" setting on a subnet?**

A. All existing instances in the subnet are assigned a public IP address.

B. Any new EC2 instance launched into that subnet will be assigned a public IP address at launch, if it has a single network interface (eth0).

C. The subnet is automatically converted to a public subnet, regardless of its route table.

D. It attaches an Internet Gateway to the VPC.

**60. You have a multi-tier web application. The web servers should be accessible from the internet, but the database servers should not. How should you configure your subnets?**

A. Place both web and database servers in a single public subnet and use security groups to restrict access to the database.

B. Place web servers in a public subnet and database servers in a private subnet.

C. Place both web and database servers in a private subnet and use a NAT Gateway for all traffic.

D. Place web servers in a private subnet and database servers in a public subnet.

**61. What is the smallest subnet you can create in a VPC?**

A. /16

B. /24

C. /28

D. /30

**62. How many usable IP addresses are in a /28 subnet?**

A. 16

B. 14

C. 11

D. 8

**63. Can a single EC2 instance have network interfaces in two different subnets?**

A. No, an instance can only exist in one subnet.

B. Yes, by attaching multiple Elastic Network Interfaces (ENIs), each in a different subnet within the same Availability Zone.

C. Yes, by attaching multiple ENIs, which can be in subnets in different Availability Zones.

D. Yes, but only if the subnets are both public.

**64. Each subnet must be associated with which of the following?**

A. A security group

B. An internet gateway

C. A route table

D. A NAT instance

**65. If you do not explicitly associate a subnet with a route table, what happens?**

A. The subnet cannot route any traffic.

B. The subnet is automatically associated with the main route table of the VPC.

C. A new, empty route table is created and associated with the subnet.

D. The subnet can only communicate with other subnets in the same Availability Zone.

**66. What is a "VPN-only subnet"?**

A. A subnet that can only be accessed via a specific security group.

B. A subnet whose associated route table directs traffic to a Virtual Private Gateway (VGW).

C. A subnet that encrypts all traffic within it by default.

D. A subnet that is not part of a VPC.

**67. You have a VPC with CIDR 172.31.0.0/16. Which of the following is a valid subnet CIDR for this VPC?**

A. 172.31.0.0/15

B. 172.32.0.0/20

C. 10.0.0.0/24

D. 172.31.16.0/20

**68. The IP address 10.0.1.2 in a /24 subnet is reserved by AWS for what purpose?**

A. VPC router

B. Amazon DNS server

C. Broadcast address

D. Network address

**69. Can you create subnets in a VPC that have overlapping CIDR blocks?**

A. Yes, but it is not recommended.

B. Yes, if they are in different Availability Zones.

C. No, all subnets within a VPC must have non-overlapping CIDR blocks.

D. No, unless you are using a Transit Gateway.

**70. To ensure high availability for an application, where should you place your subnets?**

A. All in a single, large subnet.

B. In at least two different Availability Zones.

C. In at least two different AWS Regions.

D. All in a single Availability Zone for lower latency.

**71. What is the maximum number of subnets you can create in a VPC by default?**

A. 50

B. 100

C. 200

D. 500

**72. An instance in a private subnet needs to access the internet for software updates. Which of the following is a required component in the VPC architecture?**

A. An Internet Gateway attached to the private subnet's route table.

B. An Elastic IP address attached directly to the instance.

C. A NAT Gateway or NAT Instance in a public subnet, and a route from the private subnet to it.

D. A Virtual Private Gateway.

**73. The first IP address in a subnet's CIDR block (e.g., 10.0.1.0 for 10.0.1.0/24) is reserved for what?**

A. VPC Router

B. DNS Server

C. Network Address

D. Broadcast Address

**74. The last IP address in a subnet's CIDR block (e.g., 10.0.1.255 for 10.0.1.0/24) is reserved for what?**

A. VPC Router

B. DNS Server

C. Future Use

D. Network Broadcast Address

**75. You have a subnet with CIDR 10.0.0.0/29. How many usable IP addresses are available for your instances?**

A. 8

B. 6

C. 5

D. 3

**76. Can an EC2 instance in a public subnet communicate with an EC2 instance in a private subnet within the same VPC?**

A. No, public and private subnets are isolated from each other.

B. Yes, by default, using their private IP addresses, as long as NACLs and Security Groups permit.

C. Yes, but only if a NAT Gateway is used to route the traffic.

D. Yes, but only if they are in the same Availability Zone.

**77. What is the primary difference between a public IP address and an Elastic IP address assigned to an instance in a public subnet?**

A. A public IP is static and persists through instance stops/starts, while an Elastic IP is dynamic.

B. A public IP is disassociated when an instance is stopped, while an Elastic IP remains associated with your account until you release it.

C. There is no functional difference; they are two names for the same thing.

D. Public IPs are free, while Elastic IPs always incur a charge.

**78. You want to create a subnet that is only used for IPv6 traffic. What should you do?**

A. Create a standard subnet and only launch instances with IPv6 addresses.

B. Create an IPv6-only subnet by associating an IPv6 CIDR block but no IPv4 CIDR block.

C. This is not possible; all subnets must have an IPv4 CIDR block.

D. Use an Egress-Only Internet Gateway as the subnet's primary gateway.

**79. A subnet is associated with a Network ACL. At what level does the Network ACL operate?**

A. The individual EC2 instance level.

B. The Elastic Network Interface (ENI) level.

C. The subnet level, acting as a firewall for traffic in and out of the subnet.

D. The VPC level, filtering all traffic for the entire VPC.

**80. If you launch an instance into a public subnet, does it automatically have internet access?**

A. Yes, all instances in public subnets have internet access by default.

B. No, it must also have a public IPv4 address or an Elastic IP address assigned to it.

C. No, you must first create a NAT Gateway for it.

D. Yes, but only for outbound traffic.

**81. You have two subnets, Subnet-A (10.0.1.0/24) and Subnet-B (10.0.2.0/24), in the same VPC. How is traffic routed between an instance in Subnet-A and an instance in Subnet-B?**

A. Through the Internet Gateway.

B. Through the VPC's implicit router using the 'local' route.

C. Through a NAT Gateway.

D. It requires a VPC Peering connection.

**82. What is the purpose of the "Enable resource name DNS A record on launch" subnet setting?**

A. It automatically creates a public DNS record for the instance's public IP.

B. It allows DNS queries for the instance's resource-based name to resolve to its private IPv4 address.

C. It registers the instance's name with an external DNS provider.

D. It enables DNS resolution for the entire VPC.

**83. You need to create a subnet for a service that requires a large number of IP addresses. Which CIDR block provides the most addresses?**

A. 10.0.0.0/24

B. 10.0.0.0/20

C. 10.0.0.0/16

D. 10.0.0.0/28

**84. Can a subnet span multiple Availability Zones?**

A. Yes, for high availability.

B. No, a subnet is always tied to a single Availability Zone.

C. Yes, but only in the default VPC.

D. No, unless it is a private subnet.

**85. The default subnets in a default VPC are configured to be:**

A. Private, with no internet access.

B. Public, with an attached Internet Gateway and auto-assignment of public IPs enabled.

C. A mix of one public and one private subnet per AZ.

D. VPN-only subnets.

**86. You have a subnet with the CIDR 192.168.10.0/27. What is the total number of IP addresses in this subnet?**

A. 16

B. 32

C. 64

D. 27

**87. Following the previous question, for a subnet with CIDR 192.168.10.0/27, how many IP addresses are available for you to assign to resources?**

A. 32

B. 30

C. 27

D. 29

**88. If you want to connect a subnet to the internet, but only for IPv6 traffic, what should you use?**

A. An Internet Gateway.

B. A NAT Gateway.

C. An Egress-Only Internet Gateway.

D. A Virtual Private Gateway.

**89. You have an application running on EC2 instances in a private subnet. You need these instances to be able to make API calls to an AWS service like SQS. What is the most secure and efficient way to enable this?**

A. Route traffic through a NAT Gateway in a public subnet.

B. Assign Elastic IPs to the instances and allow traffic through an Internet Gateway.

C. Create an Interface VPC Endpoint for SQS in your VPC.

D. Move the instances to a public subnet.

**90. Can you associate more than one Network ACL with a single subnet?**

A. Yes, you can associate up to 5 NACLs.

B. No, a subnet can be associated with only one Network ACL at a time.

C. Yes, one for inbound and one for outbound rules.

D. No, NACLs are associated with instances, not subnets.

**91. If a subnet is not explicitly associated with a Network ACL, what happens?**

A. All traffic is denied by default.

B. All traffic is allowed by default.

C. It becomes associated with the VPC's default Network ACL.

D. It cannot send or receive any traffic.

**92. What is the primary function of a subnet in a VPC?**

A. To provide a firewall for EC2 instances.

B. To segment the VPC's IP address range, allowing for resource isolation and route policy application.

C. To connect the VPC to the internet.

D. To assign domain names to instances.

**93. You are creating a subnet for a database that must be highly available. What is the best practice?**

A. Create one large subnet spanning multiple AZs.

B. Create separate subnets in multiple Availability Zones and deploy database replicas in each.

C. Create one subnet in a single AZ and take frequent snapshots.

D. Create one subnet and use a very large instance type for the database.

**94. The IP address 10.0.1.3 in a /24 subnet is reserved by AWS for what purpose?**

A. VPC Router

B. Amazon DNS Server

C. Reserved by AWS for future use.

D. Network Broadcast Address

**95. You have a VPC with CIDR 10.10.0.0/16. You need to create 4 subnets of equal size. Which of the following CIDR block schemes would work?**

A. 10.10.1.0/24, 10.10.2.0/24, 10.10.3.0/24, 10.10.4.0/24

B. 10.10.0.0/18, 10.10.64.0/18, 10.10.128.0/18, 10.10.192.0/18

C. 10.10.0.0/16, 10.11.0.0/16, 10.12.0.0/16, 10.13.0.0/16

D. 10.10.0.0/28, 10.10.0.16/28, 10.10.0.32/28, 10.10.0.48/28

**96. A subnet's CIDR block must be a subset of the VPC's CIDR block.**

A. True

B. False

C. Only for public subnets

D. Only for private subnets

**97. When you delete a subnet, what happens to the instances running within it?**

A. They are automatically moved to another subnet in the same AZ.

B. They are stopped.

C. You cannot delete a subnet if it contains running instances.

D. They are terminated.

**98. Which AWS service would you use to host a relational database in a private subnet?**

A. Amazon S3

B. Amazon DynamoDB

C. Amazon RDS

D. Amazon EC2 with a local database installed.

**99. If you have a subnet in us-east-1a, can an EC2 instance in that subnet have an ENI in a subnet in us-east-1b?**

A. Yes, this is a common multi-AZ setup.

B. No, all ENIs for a given instance must be in the same Availability Zone.

C. Yes, but only if using a Transit Gateway.

D. Yes, but only for specific instance types.

**100. What is the primary reason for using multiple subnets in a VPC design?**

A. To increase the total number of available IP addresses.

B. To isolate resources based on security and routing requirements (e.g., public vs. private tiers).

C. To reduce data transfer costs between instances.

D. To comply with AWS service limits.

## Route Tables

**101. What is the function of a route table in a VPC?**

A. To filter inbound and outbound traffic for a subnet.

B. To contain a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.

C. To assign IP addresses to instances.

D. To manage DNS resolution for the VPC.

**102. Every VPC has a _____ route table that is created automatically when the VPC is created.**

A. primary

B. default

C. main

D. custom

**103. What is the "local" route that exists in every route table by default?**

A. A route to the internet (0.0.0.0/0).

B. A route that enables communication within the VPC.

C. A route to your on-premises network.

D. A route to the Amazon DNS server.

**104. Can you delete the main route table of a VPC?**

A. Yes, if no subnets are associated with it.

B. Yes, but a new main route table must be designated immediately.

C. No, you cannot delete the main route table.

D. No, but you can replace all of its routes.

**105. What is a "custom route table"?**

A. The main route table after you have modified it.

B. Any route table that you create for your VPC.

C. A route table that only contains routes to on-premises networks.

D. A route table that cannot be modified.

**106. To make a subnet a "public subnet," you must add a route to what type of target in its associated route table?**

A. A NAT Gateway

B. A Virtual Private Gateway

C. An Internet Gateway

D. A VPC Endpoint

**107. What is the destination for a route that directs traffic to the internet?**

A. 10.0.0.0/8

B. The VPC's CIDR block

C. 0.0.0.0/0

D. The subnet's CIDR block

**108. A subnet can be associated with how many route tables at a time?**

A. Zero

B. Exactly one

C. One for inbound and one for outbound

D. Up to five

**109. A route table can be associated with how many subnets?**

A. Exactly one

B. Zero

C. One or more

D. A maximum of five

**110. If a subnet is not explicitly associated with any route table, which route table does it use?**

A. It uses a new, empty route table created for it.

B. It cannot route traffic outside of the subnet.

C. It uses the VPC's main route table.

D. The launch of instances into that subnet will fail.

**111. You have a private subnet (Subnet-A) and a public subnet (Subnet-B). An instance in Subnet-A needs to download a patch from the internet. You have a NAT Gateway in Subnet-B. What route must be present in the route table for Subnet-A?**

A. Destination: 0.0.0.0/0, Target: Internet Gateway

B. Destination: 0.0.0.0/0, Target: NAT Gateway

C. Destination: VPC CIDR, Target: local

D. Destination: NAT Gateway IP, Target: Internet Gateway

**112. What does "route propagation" in a route table do?**

A. It automatically copies routes from the main route table to all custom route tables.

B. It allows a Virtual Private Gateway (VGW) to automatically propagate routes from your on-premises network to your route table.

C. It propagates DNS settings throughout the VPC.

D. It shares routes between peered VPCs.

**113. When multiple routes match a packet's destination, how does the VPC router decide which route to use?**

A. It uses the route with the lowest metric.

B. It uses the most specific route (the one with the longest prefix).

C. It load balances the traffic across all matching routes.

D. It uses the oldest route that was added.

**114. You have a route to 172.31.0.0/16 via a VPC peering connection and another route to 172.31.1.0/24 via a VPN gateway. Where will traffic destined for 172.31.1.5 be sent?**

A. To the VPC peering connection, because it has a larger CIDR block.

B. To the VPN gateway, because its route (172.31.1.0/24) is more specific.

C. The traffic will be dropped because of a routing conflict.

D. The traffic will be load-balanced between the two targets.

**115. Can you modify the "local" route in a route table?**

A. Yes, you can change its target.

B. Yes, you can delete it.

C. No, the local route cannot be modified or deleted.

D. Yes, but only in the main route table.

**116. You have set up a Gateway VPC Endpoint for Amazon S3. What change is automatically made to your route table?**

A. A route for 0.0.0.0/0 is added with the endpoint as the target.

B. A route is added for the public IP range of S3, with the VPC endpoint as the target.

C. The 'local' route is modified to include the S3 endpoint.

D. No changes are made to the route table; endpoints work at the DNS level.

**117. What is the target for a route that directs traffic to a VPC peering connection?**

A. The peering connection ID (e.g., pcx-12345678).

B. The CIDR block of the peered VPC.

C. The Internet Gateway of the peered VPC.

D. The Virtual Private Gateway of the peered VPC.

**118. You want to replace the main route table with a custom route table you have created. What is the procedure?**

A. Delete the current main route table, which automatically promotes a custom one.

B. In the VPC settings, there is an option to "Swap Main Route Table".

C. You explicitly associate your custom route table to be the new main route table in the "Route Tables" section of the VPC console.

D. This is not possible; the original main route table is permanent.

**119. What is the purpose of an "edge association" in a route table?**

A. To associate a route table with a subnet near the edge of the AWS network.

B. To associate a route table with an Internet Gateway or Virtual Private Gateway to route inbound traffic.

C. To connect a route table to an AWS WAF rule.

D. To link a route table to a CloudFront distribution.

**120. A route in a route table has a status of "blackhole". What does this mean?**

A. The route is active and functioning correctly.

B. The route's target is not currently available (e.g., a terminated instance or detached gateway), and traffic going to that route will be dropped.

C. The route is configured to intentionally drop all matching traffic.

D. The route is propagating from a VPN connection.

**121. To allow instances in a private subnet to communicate with on-premises servers over a Site-to-Site VPN connection, what route is needed in the private subnet's route table?**

A. Destination: 0.0.0.0/0, Target: Virtual Private Gateway (VGW)

B. Destination: On-premises network CIDR, Target: Virtual Private Gateway (VGW)

C. Destination: On-premises network CIDR, Target: Internet Gateway (IGW)

D. Destination: 0.0.0.0/0, Target: NAT Gateway

**122. Can a route table have routes to both an Internet Gateway and a Virtual Private Gateway?**

A. No, a route table can only point to one type of gateway.

B. Yes, this is a common configuration for subnets that need access to both the internet and an on-premises network.

C. Yes, but only if the destinations are non-overlapping.

D. No, this would create a routing loop.

**123. What is the target for a route that directs IPv6 traffic to the internet?**

A. An Internet Gateway (IGW).

B. A NAT Gateway.

C. An Egress-Only Internet Gateway.

D. A Virtual Private Gateway (VGW).

**124. The destination for an IPv6 internet-bound route is:**

A. 0.0.0.0/0

B. ::/0

C. The specific IPv6 address of the destination.

D. The IPv6 CIDR of the VPC.

**125. You have a route table associated with three subnets. If you add a new route to this table, how many subnets are affected?**

A. None, the change must be propagated manually.

B. Only the first subnet in the association list.

C. All three subnets.

D. A new route table is created, and the subnets must be re-associated.

**126. What is the maximum number of routes you can have in a route table by default?**

A. 20

B. 50

C. 100

D. 200

**127. You have configured a Transit Gateway and attached your VPC to it. To route traffic from your VPC to another VPC through the Transit Gateway, what must you do in your subnet's route table?**

A. Add a route for the destination VPC's CIDR with the target set to the Transit Gateway ID.

B. Enable route propagation from the Transit Gateway.

C. Add a route for 0.0.0.0/0 with the target set to the Transit Gateway ID.

D. Create a VPC peering connection as a backup.

**128. Which of the following is NOT a valid target for a route in a VPC route table?**

A. Internet Gateway

B. NAT Gateway

C. Security Group

D. VPC Peering Connection

**129. You have a main route table with a route to an Internet Gateway. You also have a custom route table with no internet route, associated with a specific subnet. Is this subnet public or private?**

A. Public, because the main route table has an internet route.

B. Private, because its explicit route table association determines its routing path.

C. It is both public and private.

D. It depends on the security group configuration.

**130. To route traffic from your VPC to an on-premises network through an AWS Direct Connect connection, the route target in your route table would be a:**

A. Internet Gateway

B. Virtual Private Gateway

C. NAT Gateway

D. Transit Gateway

**131. Can you have a route with a destination that is a single IP address (e.g., 52.95.110.82/32)?**

A. No, routes must be CIDR blocks of /28 or larger.

B. Yes, this is a valid way to create a highly specific route, often used for routing to a specific host.

C. No, this is not a valid CIDR notation.

D. Yes, but only for targets within the same VPC.

**132. What is the primary difference in function between a route table and a network ACL?**

A. Route tables are stateful, NACLs are stateless.

B. Route tables direct traffic, while NACLs permit or deny traffic.

C. Route tables operate at the instance level, NACLs at the subnet level.

D. There is no functional difference.

**133. You have created a new VPC from scratch. What routes will the main route table contain initially?**

A. Only the 'local' route for the VPC's CIDR.

B. A 'local' route and a route to 0.0.0.0/0 via an Internet Gateway.

C. An empty route table.

D. A 'local' route and a route to the Amazon DNS server.

**134. If you disassociate a custom route table from a subnet, what happens to the subnet's routing?**

A. It loses all routing capabilities.

B. It automatically associates with the VPC's main route table.

C. It retains a cached copy of the custom route table's routes.

D. All instances in the subnet are terminated.

**135. A route table for a private subnet needs to allow instances to access Amazon S3 without going over the internet. What should the route table contain?**

A. A route to 0.0.0.0/0 targeting a NAT Gateway.

B. A route to the S3 prefix list ID targeting a Gateway VPC Endpoint.

C. A route to 0.0.0.0/0 targeting an Internet Gateway.

D. A route to the S3 prefix list ID targeting a Virtual Private Gateway.

**136. Which of the following is a valid target for a route in a route table?**

A. An EC2 Instance ID

B. An Elastic IP Address

C. An Elastic Network Interface (ENI) ID

D. An S3 Bucket Name

**137. You are troubleshooting a connectivity issue. An instance in a public subnet cannot reach the internet. You have confirmed it has a public IP and its security group allows outbound traffic. What is the next most likely component to check?**

A. The DHCP Options Set.

B. The route table associated with the subnet for a route to the Internet Gateway.

C. The Network ACL for an outbound deny rule.

D. The VPC's tenancy attribute.

**138. Can a route table associated with a subnet in Availability Zone A have a route to a NAT Gateway located in Availability Zone B?**

A. No, the NAT Gateway must be in the same AZ as the subnet.

B. Yes, this is a common and valid configuration.

C. Yes, but it will result in higher latency and cross-AZ data transfer charges.

D. No, this would require a VPC peering connection.

**139. What is the purpose of associating a route table with a gateway (a "gateway route table")?**

A. To control routing for traffic originating from the gateway itself.

B. It's another name for the main route table.

C. To control the routing path for traffic that enters your VPC through that gateway.

D. This is not a valid concept in AWS VPC.

**140. You have a route table with two routes: Destination 0.0.0.0/0 -> IGW and Destination 10.0.0.0/8 -> VGW. An instance sends a packet to 8.8.8.8. Which route is used?**

A. The route to the VGW because it was added first.

B. The route to the IGW because 8.8.8.8 falls within 0.0.0.0/0.

C. The traffic is dropped due to ambiguity.

D. The route to the VGW because it is more specific.

**141. You have a route table with two routes: Destination 192.168.1.0/24 -> pcx-1 and Destination 192.168.0.0/16 -> pcx-2. An instance sends a packet to 192.168.1.50. Which route is used?**

A. The route to pcx-2, because its CIDR range is larger.

B. The route to pcx-1, because its prefix (/24) is longer and therefore more specific.

C. The traffic is load balanced between pcx-1 and pcx-2.

D. The traffic is dropped because of the overlapping CIDR blocks.

**142. Can you create a route that directs traffic from your VPC back to itself (a loop)?**

A. Yes, but the route will show a "blackhole" status.

B. No, the VPC router prevents the creation of such routes.

C. Yes, this is a valid technique for traffic inspection.

D. Only if using a Transit Gateway.

**143. The routes learned via BGP from a Direct Connect or VPN connection can be automatically added to a route table by enabling what feature?**

A. Route Propagation

B. Route Aggregation

C. Route Reflection

D. Route Injection

**144. What is the key difference between the main route table and a custom route table in terms of default behavior?**

A. The main route table cannot be modified.

B. Custom route tables are associated with new subnets by default.

C. The main route table is associated with any subnet that doesn't have an explicit association; custom route tables are not.

D. Custom route tables have higher priority than the main route table.

**145. To provide outbound-only internet access for IPv6 instances in a private subnet, you would add a route of ::/0 to what target?**

A. NAT Gateway

B. Internet Gateway

C. Egress-Only Internet Gateway

D. Virtual Private Gateway

**146. You have peered VPC-A and VPC-B. To allow an instance in VPC-A to communicate with an instance in VPC-B, what is required in VPC-A's route table?**

A. A route with the destination of VPC-B's CIDR and the target of the VPC peering connection ID.

B. A route with the destination of 0.0.0.0/0 and the target of the VPC peering connection ID.

C. No route is needed; peering is automatic.

D. A route with the destination of VPC-B's CIDR and the target of VPC-A's Internet Gateway.

**147. Which of the following is a key principle of VPC routing?**

A. Least specific prefix match

B. Round-robin routing

C. Most specific prefix match (longest prefix match)

D. Lowest metric routing

**148. You have a NAT Instance (an EC2 instance) with ID i-12345. How would you route traffic from a private subnet to it?**

A. Destination: 0.0.0.0/0, Target: i-12345

B. Destination: 0.0.0.0/0, Target: The ENI ID of the NAT instance

C. Destination: 0.0.0.0/0, Target: The private IP of the NAT instance

D. You cannot route to an EC2 instance directly; you must use a NAT Gateway.

**149. If you change the main route table, which subnets are immediately affected?**

A. All subnets in the VPC.

B. Only the subnets that are explicitly associated with the main route table.

C. Only the subnets that do not have a custom route table association.

D. No subnets are affected until the changes are propagated.

**150. A route table is a regional resource.**

A. True. It can be associated with subnets in any AZ within its region.

B. False. A route table is scoped to an Availability Zone.

C. False. A route table is a global resource.

D. True, but it can only be associated with subnets in one AZ at a time.

## Internet Gateways (IGW)

**151. What is the primary function of an Internet Gateway (IGW)?**

A. To provide a target in your VPC route tables for internet-routable traffic.

B. To filter traffic between subnets in a VPC.

C. To connect a VPC to an on-premises data center.

D. To provide private, dedicated access to AWS services.

**152. An Internet Gateway is a resource that is...**

A. Zonally redundant by default.

B. Regionally redundant by default.

C. Horizontally scaled, redundant, and highly available.

D. A single point of failure unless you deploy two of them.

**153. How many Internet Gateways can be attached to a single VPC at a time?**

A. One

B. Two, for redundancy

C. One per Availability Zone

D. As many as you need

**154. To enable internet access for a VPC, what are the three main steps required?**

A. Create a NAT Gateway, attach it to the VPC, and add a route to it.

B. Create an IGW, attach it to the VPC, and add a route (0.0.0.0/0) to the route table pointing to the IGW.

C. Create a public subnet, launch an instance, and assign an Elastic IP.

D. Enable DNS hostnames, enable DNS resolution, and create a security group.

**155. An EC2 instance in a public subnet needs to be reachable from the internet. Besides a route to the IGW, what else must the instance have?**

A. A private IP address only.

B. A public IPv4 address or an Elastic IP address.

C. A connection to a NAT Gateway.

D. An IAM role with internet access permissions.

**156. Does an Internet Gateway impose any bandwidth constraints on your internet traffic?**

A. Yes, it is limited to 1 Gbps by default.

B. Yes, it is limited to 5 Gbps by default.

C. No, it is a horizontally scaled component and does not impose bandwidth constraints.

D. Yes, the bandwidth is determined by the instance type of the gateway.

**157. If you detach an Internet Gateway from your VPC, what is the immediate effect?**

A. All instances in the VPC lose their private IP addresses.

B. Resources in public subnets lose their internet access.

C. The main route table is deleted.

D. All running instances in the VPC are terminated.

**158. An Internet Gateway performs 1:1 NAT for instances that have been assigned what?**

A. A private IPv4 address only.

B. A public IPv4 address or an Elastic IP address.

C. An IPv6 address.

D. A secondary private IP address.

**159. Can an Internet Gateway be shared between multiple VPCs?**

A. Yes, using VPC sharing.

B. No, an IGW is dedicated to a single VPC.

C. Yes, by using a Transit Gateway.

D. No, but you can peer the VPCs to share one IGW.

**160. What is the difference between an Internet Gateway and a NAT Gateway?**

A. An IGW allows inbound/outbound internet access for public subnets, while a NAT Gateway allows outbound-only internet access for private subnets.

B. An IGW is for IPv4, and a NAT Gateway is for IPv6.

C. An IGW is a physical device, while a NAT Gateway is a managed service.

D. There is no difference; they are interchangeable.

**161. To create a public subnet, you must update the subnet's route table to point internet-bound traffic to the...**

A. Virtual Private Gateway

B. NAT Gateway

C. Internet Gateway

D. Local Router

**162. Is there a data processing charge for traffic that goes through an Internet Gateway?**

A. Yes, for all inbound and outbound traffic.

B. No, there is no charge for the IGW itself or for data transfer through it, but standard EC2 data transfer out charges apply.

C. Yes, there is a fixed hourly charge for having an IGW attached.

D. No, all traffic through an IGW is free.

**163. An Internet Gateway supports both IPv4 and IPv6 traffic.**

A. True

B. False

C. Only for default VPCs

D. Only when used with a Transit Gateway

**164. You have created and attached an IGW to your VPC. However, instances in your public subnet still cannot access the internet. What is the most likely missing step?**

A. The instances do not have public IP addresses.

B. The subnet's route table does not have a route to the IGW.

C. The security group is blocking outbound traffic.

D. Any of the above could be the cause.

**165. What is the state of an Internet Gateway before it is attached to a VPC?**

A. attached

B. pending

C. detached

D. unavailable

**166. An Internet Gateway is required for which of the following scenarios?**

A. Communication between two private subnets in the same VPC.

B. An EC2 instance in a public subnet to be reached from the internet.

C. An EC2 instance in a private subnet to reach an on-premises server via VPN.

D. An EC2 instance to communicate with an S3 bucket via a Gateway Endpoint.

**167. What does it mean that an IGW is a "horizontally scaled" component?**

A. You must add more IGWs to get more bandwidth.

B. It automatically scales to handle the amount of traffic, so it's not a bottleneck.

C. It scales by increasing the EC2 instance size it runs on.

D. It can only scale up, not down.

**168. Can you control traffic passing through an Internet Gateway using Security Groups?**

A. Yes, you can attach a Security Group directly to the IGW.

B. No, Security Groups apply to ENIs/instances, not the IGW itself. Traffic is filtered at the instance.

C. Yes, but only for inbound traffic.

D. No, you must use Network ACLs for this.

**169. An Egress-Only Internet Gateway is for _____ traffic, while a standard Internet Gateway is for _____ traffic.**

A. IPv4; IPv6

B. outbound IPv6; bidirectional IPv4 and IPv6

C. inbound only; outbound only

D. VPN; public internet

**170. If you delete a VPC, what happens to the Internet Gateway that was attached to it?**

A. It is automatically detached and remains in your account in a 'detached' state.

B. It is automatically deleted.

C. It is moved to the default VPC.

D. You cannot delete a VPC with an IGW attached.

**171. An Internet Gateway provides a 1:1 NAT translation between a private IPv4 address and a public/Elastic IPv4 address. Where does this translation happen?**

A. On the EC2 instance itself.

B. At the subnet router.

C. At the Internet Gateway.

D. At the Network ACL.

**172. Which of the following is a key characteristic of an Internet Gateway?**

A. It is a managed EC2 instance that you must patch.

B. It is a single point of failure for internet connectivity.

C. It provides fault tolerance and high availability without any user management.

D. It can only be used with the default VPC.

**173. You have an EC2 instance with only a private IP in a subnet that has a route to an IGW. Can this instance access the internet?**

A. Yes, the IGW will perform NAT for it.

B. No, the instance must have a public or Elastic IP for the IGW to perform the required 1:1 NAT.

C. Yes, but only for outbound traffic.

D. No, the route table is invalid in this configuration.

**174. What is the target specified in a route table for internet-bound IPv4 traffic?**

A. The ID of the Internet Gateway (e.g., igw-xxxxxxxx).

B. The public IP address of the Internet Gateway.

C. The string "internet".

D. The CIDR block of the public subnet.

**175. An Internet Gateway is a regional service. This means:**

A. It can connect VPCs across different regions.

B. It exists within a region and is resilient to the failure of a single Availability Zone.

C. It is a global service like IAM or Route 53.

D. You need to specify an Availability Zone when creating it.

**176. What is the purpose of an Egress-Only Internet Gateway?**

A. To allow instances in a private subnet to initiate outbound connections to the internet over IPv6, but prevent the internet from initiating connections to those instances.

B. To filter all outbound traffic from a VPC.

C. To provide a cheaper alternative to a standard Internet Gateway.

D. To allow outbound connections over IPv4 only.

**177. How is an Egress-Only Internet Gateway different from a NAT Gateway?**

A. An Egress-Only IGW is for IPv6, while a NAT Gateway is for IPv4.

B. A NAT Gateway is for IPv6, while an Egress-Only IGW is for IPv4.

C. They are functionally identical but have different pricing.

D. An Egress-Only IGW is stateful, while a NAT Gateway is stateless.

**178. To use an Egress-Only Internet Gateway, what route must you add to your private subnet's route table?**

A. Destination: 0.0.0.0/0, Target: Egress-Only IGW ID

B. Destination: ::/0, Target: Egress-Only IGW ID

C. Destination: ::/0, Target: Internet Gateway ID

D. Destination: 0.0.0.0/0, Target: NAT Gateway ID

**179. Can you attach an Egress-Only Internet Gateway to a VPC that does not have an IPv6 CIDR block associated with it?**

A. Yes, it will handle IPv4 traffic as well.

B. No, Egress-Only IGWs are specifically for IPv6 and require the VPC to be IPv6-enabled.

C. Yes, but it will have no effect.

D. No, you must attach a standard IGW first.

**180. Like a standard Internet Gateway, an Egress-Only Internet Gateway is a highly available, managed AWS component.**

A. True

B. False

C. True, but it is not redundant.

D. False, it is a single EC2 instance you must manage.

## NAT Gateway / NAT Instance

**181. What is the primary purpose of a NAT Gateway?**

A. To allow instances in a public subnet to communicate with the internet.

B. To enable instances in a private subnet to initiate outbound IPv4 traffic to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

C. To connect two VPCs together.

D. To provide a secure, private connection to AWS services like S3.

**182. In which type of subnet must a NAT Gateway be placed?**

A. A private subnet

B. A public subnet

C. A VPN-only subnet

D. It can be placed in any subnet.

**183. To function correctly, a NAT Gateway requires what type of IP address to be associated with it?**

A. A private IP address only

B. An Elastic IP address

C. A secondary private IP address

D. An IPv6 address

**184. What is a key difference between a NAT Gateway and a NAT Instance regarding high availability?**

A. A NAT Gateway is managed by AWS and is redundant within an Availability Zone, while a NAT Instance is a single EC2 instance that can be a single point of failure.

B. A NAT Instance is more highly available than a NAT Gateway.

C. Both are equally highly available.

D. A NAT Gateway must be deployed in pairs for high availability, while a NAT Instance is automatically redundant.

**185. What is a key difference between a NAT Gateway and a NAT Instance regarding bandwidth?**

A. A NAT Instance's bandwidth is determined by its instance type, while a NAT Gateway can scale up to 45 Gbps.

B. A NAT Gateway's bandwidth is fixed at 5 Gbps, while a NAT Instance can scale higher.

C. Both have identical bandwidth capabilities.

D. A NAT Gateway has lower latency but less bandwidth than a large NAT Instance.

**186. You have configured a NAT Instance. What critical setting must be disabled on the EC2 instance for it to work correctly?**

A. Termination Protection

B. Detailed Monitoring

C. Source/Destination Check

D. Auto-assign Public IP

**187. To route traffic from a private subnet to a NAT Gateway, what entry should be in the private subnet's route table?**

A. Destination: 0.0.0.0/0, Target: The NAT Gateway's ID (nat-xxxxxxxx)

B. Destination: 0.0.0.0/0, Target: The Internet Gateway's ID (igw-xxxxxxxx)

C. Destination: The VPC's CIDR, Target: local

D. Destination: The NAT Gateway's private IP, Target: local

**188. Can you associate a Security Group with a NAT Gateway?**

A. Yes, it is a required step.

B. No, you cannot associate a Security Group directly with a NAT Gateway.

C. Yes, but only to control outbound traffic.

D. No, you must use a Network ACL instead.

**189. How do you achieve a highly available architecture for internet access from private subnets across multiple Availability Zones using NAT Gateways?**

A. Deploy a single, large NAT Gateway in one AZ and route all traffic to it.

B. Deploy a NAT Gateway in each Availability Zone and configure route tables so that resources use the NAT Gateway in their own AZ.

C. Deploy a NAT Gateway and a NAT Instance as a failover pair.

D. Use a Transit Gateway to manage a single NAT Gateway for all AZs.

**190. Which of the following is a responsibility you have when using a NAT Instance, but not when using a NAT Gateway?**

A. Associating an Elastic IP address.

B. Updating the route tables to use it.

C. Managing OS patching, security updates, and instance scaling.

D. Paying for data processing.

**191. A NAT Gateway supports which type of traffic?**

A. IPv4 only

B. IPv6 only

C. Both IPv4 and IPv6

D. TCP only

**192. For outbound-only internet access for IPv6 traffic from a private subnet, what should you use?**

A. A NAT Gateway

B. A NAT Instance

C. An Egress-Only Internet Gateway

D. An Internet Gateway

**193. What happens to a NAT Gateway if the Elastic IP associated with it is disassociated?**

A. It continues to function using a new, automatically assigned public IP.

B. It stops being able to route traffic to the internet.

C. It is automatically terminated.

D. It switches to a failover NAT Gateway in another AZ.

**194. When comparing cost, a NAT Instance can be cheaper than a NAT Gateway for...**

A. High-bandwidth, constant workloads.

B. Very low-traffic or bursty workloads, especially if a t-series instance is used.

C. NAT Gateways are always cheaper than NAT Instances.

D. Workloads that span multiple Availability Zones.

**195. Can a NAT Instance be used to port forward inbound traffic to an instance in a private subnet?**

A. No, NAT Instances only handle outbound traffic.

B. Yes, by configuring iptables rules on the NAT Instance, it can be used for port forwarding, although this is a complex setup.

C. Yes, AWS provides a simple "port forwarding" checkbox for NAT Instances.

D. No, only a NAT Gateway can do this.

**196. When creating a NAT Gateway, you must specify:**

A. The private subnet it will serve.

B. The public subnet it will reside in and an Elastic IP to associate with it.

C. The instance type to use for the gateway.

D. The security group to attach to it.

**197. A NAT Gateway is a resource that is specific to a single:**

A. Region

B. VPC

C. Subnet

D. Availability Zone

**198. If the NAT Gateway in AZ-A fails, what happens to instances in a private subnet in AZ-A that are routed to it?**

A. AWS automatically fails over to a standby NAT Gateway in the same AZ.

B. Traffic is automatically rerouted to a NAT Gateway in another AZ.

C. They lose internet connectivity until the NAT Gateway is restored or the route is changed.

D. The instances are terminated.

**199. What is the main advantage of using a NAT Gateway over a NAT Instance?**

A. Lower cost for all use cases.

B. Reduced operational overhead, as it's a managed service.

C. Ability to act as a bastion host.

D. Support for IPv6 traffic.

**200. You are using a NAT Instance. To allow traffic from your private subnets to reach it, what must you configure on the NAT Instance's Security Group?**

A. Allow all traffic from 0.0.0.0/0.

B. Allow inbound HTTP/HTTPS traffic from the CIDR block of your private subnets.

C. Allow all outbound traffic to 0.0.0.0/0.

D. Security groups do not apply to NAT Instances.

**201. A NAT Gateway translates the source private IP of instances to what IP address before sending traffic to the internet?**

A. The private IP address of the NAT Gateway.

B. The Elastic IP address of the NAT Gateway.

C. A random IP from a pool owned by AWS.

D. The private IP address of the Internet Gateway.

**202. Can a single NAT Gateway serve multiple private subnets?**

A. No, you need one NAT Gateway per private subnet.

B. Yes, as long as the route tables for those subnets point to it.

C. Yes, but only if the subnets are in the same Availability Zone as the NAT Gateway.

D. Yes, and it's a best practice to have subnets in different AZs point to a single NAT Gateway for cost savings.

**203. Why is it a best practice to have a NAT Gateway in each AZ rather than routing cross-AZ to a single NAT Gateway?**

A. To avoid inter-AZ data transfer costs and improve resilience.

B. Because a NAT Gateway can only route traffic for its own AZ.

C. To increase the total available bandwidth.

D. Because AWS billing requires it.

**204. If you are using a NAT Instance, who is responsible for right-sizing the instance for your traffic needs?**

A. AWS Support

B. The user/administrator

C. It is automatically scaled by AWS.

D. The instance size is fixed and cannot be changed.

**205. A NAT Gateway is stateful. What does this mean for return traffic?**

A. Return traffic is automatically allowed back to the instance that initiated the connection.

B. You must create a Network ACL rule to allow the return traffic.

C. You must create a Security Group rule to allow the return traffic.

D. Return traffic is blocked by default.

**206. Which of the following is a valid use case for a NAT Gateway?**

A. Allowing a user on the internet to SSH into a private EC2 instance.

B. Allowing a private EC2 instance to download updates from an internet repository.

C. Allowing two private EC2 instances in different VPCs to communicate.

D. Allowing a public EC2 instance to host a website.

**207. When you create a NAT Gateway, its network interface is created in which subnet?**

A. The private subnet that will use it.

B. The public subnet that you specify during creation.

C. A special, AWS-managed subnet.

D. The subnet associated with the main route table.

**208. To create a NAT Instance, you typically use a specific AMI that is pre-configured for NAT.**

A. True

B. False

C. True, but you can also configure any standard Linux AMI manually.

D. False, you must build it from scratch every time.

**209. What happens if the public subnet containing your only NAT Gateway has its route to the Internet Gateway removed?**

A. The NAT Gateway will fail over to another AZ.

B. The NAT Gateway will stop working, and all private instances using it will lose internet access.

C. The NAT Gateway will automatically create a new route.

D. Traffic will be unaffected.

**210. Can a NAT Gateway be the target of a route from a public subnet's route table?**

A. Yes, this is a common configuration.

B. No, this would create a routing loop as the NAT Gateway itself needs a route to the IGW.

C. Yes, but it is not recommended.

D. Only if the NAT Gateway is in a different VPC.

**211. What is the key security benefit of using a NAT Gateway for private instances?**

A. It encrypts all traffic to the internet.

B. It prevents unsolicited inbound connections from the internet.

C. It performs deep packet inspection on all traffic.

D. It integrates with AWS WAF for application-layer filtering.

**212. If you terminate the EC2 instance being used as a NAT Instance, what must you do to restore connectivity for your private subnets?**

A. The system will auto-heal and launch a new one.

B. You must launch a new NAT Instance and update the route tables to point to the new instance's ENI or IP.

C. You only need to update the route table; the instance will be replaced automatically.

D. You must contact AWS support to restore the instance.

**213. A NAT Gateway is billed based on which two factors?**

A. The number of routes pointing to it and the amount of data processed.

B. An hourly charge for being provisioned and a per-GB charge for data processed.

C. The instance type and the amount of data transferred out.

D. The number of associated Elastic IPs and the number of active connections.

**214. Why must Source/Destination Check be disabled for a NAT Instance?**

A. To allow the instance to receive traffic destined for its own IP address.

B. To allow the instance to send and receive traffic when the source or destination is not itself.

C. To enable detailed monitoring.

D. To allow it to be associated with an Elastic IP.

**215. Can you use a NAT Gateway to provide internet access for an on-premises network connected via Direct Connect?**

A. Yes, by routing traffic from on-premises to the NAT Gateway.

B. No, a NAT Gateway can only be used by resources within its VPC.

C. Yes, but only if using a Transit Gateway.

D. No, you must use your own on-premises NAT solution.

**216. A NAT Gateway supports a maximum of 55,000 concurrent connections to each unique destination. What happens if this limit is exceeded?**

A. The NAT Gateway scales automatically to support more connections.

B. New connections to that destination will fail.

C. The NAT Gateway will fail and need to be replaced.

D. Older connections are dropped to make room for new ones.

**217. Which component is NOT required for a private instance to access the internet via a NAT Gateway?**

A. A route in the private subnet's route table pointing 0.0.0.0/0 to the NAT Gateway.

B. A NAT Gateway in a public subnet.

C. An Internet Gateway attached to the VPC.

D. An Elastic IP attached to the private instance.

**218. A NAT Instance can also function as a bastion (jump) host, whereas a NAT Gateway cannot.**

A. True, because a NAT Instance is a regular EC2 instance you can SSH into.

B. False, a NAT Gateway can also be configured as a bastion host.

C. False, neither can be used as a bastion host.

D. True, but it is not a recommended security practice.

**219. If you delete a NAT Gateway, what happens to the Elastic IP that was associated with it?**

A. The EIP is also deleted.

B. The EIP is disassociated and remains in your account.

C. The EIP is attached to the Internet Gateway.

D. The EIP is released back to the public pool.

**220. A company wants the simplest, most managed solution for providing internet access to its private EC2 instances. What should they choose?**

A. A fleet of auto-scaling NAT Instances.

B. A NAT Gateway.

C. An Egress-Only Internet Gateway.

D. A custom proxy solution on EC2.

**221. A NAT Gateway is created in a specific Availability Zone. Can it fail over to another AZ automatically?**

A. Yes, it has automatic cross-AZ failover.

B. No, a NAT Gateway is resilient within its AZ, but does not automatically fail over to another AZ.

C. Yes, if you configure it with a failover IP.

D. No, because NAT Gateways are a regional service.

**222. When using a NAT Instance, you are responsible for managing its security group. What is a reasonable inbound rule for this security group?**

A. Allow All Traffic from 0.0.0.0/0.

B. Allow All Traffic from the CIDR range of your private subnets.

C. Deny All Traffic.

D. Allow SSH from your corporate IP and HTTP/HTTPS from your private subnets.

**223. A NAT Gateway does not support port forwarding.**

A. True. It is used for outbound traffic only.

B. False. It can be configured for port forwarding via the VPC console.

C. True, unless it is paired with an Application Load Balancer.

D. False, it supports port forwarding for TCP traffic but not UDP.

**224. What is the target in a route table when using a NAT Instance?**

A. The instance ID of the NAT Instance.

B. The private IP address of the NAT Instance.

C. The Elastic IP address of the NAT Instance.

D. The Network Interface ID (ENI) of the NAT Instance.

**225. You have a private subnet in us-east-1a and a NAT Gateway in us-east-1b. What is a potential downside of this configuration?**

A. This configuration is not possible.

B. It will not work because of routing limitations.

C. You will incur cross-AZ data transfer charges for traffic going through the NAT Gateway.

D. The latency will be unacceptably high for all applications.

**226. A NAT Gateway is preferred over a NAT Instance for enterprise workloads primarily due to its...**

A. Lower cost and better performance.

B. Higher bandwidth, managed nature, and built-in redundancy.

C. Ability to be customized with additional software.

D. Support for more protocols.

**227. If a NAT Gateway's status shows as 'failed', what is the recommended first step?**

A. Reboot the gateway.

B. Delete the failed NAT Gateway and create a new one.

C. Contact AWS Support immediately.

D. Check the route tables for errors.

**228. Can a NAT Gateway function without an Internet Gateway in the VPC?**

A. Yes, it can route traffic between private subnets.

B. No, a NAT Gateway needs a route to an Internet Gateway to send traffic to the internet.

C. Yes, it has its own built-in connection to the internet.

D. No, unless it is routing to a Virtual Private Gateway.

**229. Which of these is NOT a feature of a NAT Gateway?**

A. Managed by AWS

B. Scales up to 45 Gbps

C. Can be used as a bastion host

D. Redundant within an Availability Zone

**230. To use a NAT Instance, you must select an AMI that is configured to perform NAT. This typically involves what underlying OS feature?**

A. DNS forwarding

B. IP forwarding (or IP masquerading)

C. A web server like Apache

D. A database like MySQL

**231. A NAT Gateway uses which of the following to keep track of sessions?**

A. A state table that maps outbound connections to the originating private instance.

B. Security group connection tracking.

C. Network ACL rules.

D. A DynamoDB table.

**232. You have a high-availability setup with a NAT Gateway in each of two AZs. The NAT Gateway in AZ-A fails. What happens to instances in AZ-B?**

A. They also lose internet connectivity.

B. Their traffic is unaffected, as they should be routed to the NAT Gateway in their own AZ (AZ-B).

C. Their traffic is automatically rerouted to the failed NAT Gateway in AZ-A.

D. They are terminated to prevent errors.

**233. A NAT Instance requires more security-related management than a NAT Gateway because...**

A. It is not managed by AWS, so you are responsible for patching the OS and managing its security group.

B. It processes more sensitive data.

C. It does not support encryption.

D. It is always placed in a less secure subnet.

**234. If you need to provide internet access to thousands of instances in a private subnet with very high, bursty bandwidth needs, which is the better choice?**

A. A NAT Instance, because you can choose a large, network-optimized instance type.

B. A NAT Gateway, because it is managed and scales automatically to handle high bandwidth.

C. Multiple NAT Instances behind a load balancer.

D. An Egress-Only Internet Gateway.

**235. Can you change the Elastic IP address of a NAT Gateway after it has been created?**

A. Yes, through the "Modify NAT Gateway" option.

B. No, you must create a new NAT Gateway with the desired EIP and update your route tables.

C. Yes, by disassociating the old EIP and associating a new one.

D. No, the EIP is permanently tied to the NAT Gateway.

**236. A NAT Gateway is a form of...**

A. Port Address Translation (PAT).

B. 1-to-1 NAT.

C. Static NAT.

D. DNS-based NAT.

**237. When using a NAT Instance, what is a common way to achieve high availability?**

A. Use a very large instance type that will not fail.

B. Use a script that monitors the primary NAT Instance and, upon failure, automatically remaps routes to a standby NAT Instance.

C. NAT Instances are highly available by default.

D. Place the NAT Instance behind an Application Load Balancer.

**238. A NAT Gateway helps private instances by hiding their private IP addresses from the internet.**

A. True

B. False

C. Only for TCP traffic

D. Only when used with a NAT Instance

**239. Which of the following is a drawback of using a NAT Instance compared to a NAT Gateway?**

A. It does not support IPv4.

B. It represents a potential administrative burden for patching and maintenance.

C. It cannot be used in a custom VPC.

D. It is always more expensive.

**240. You have an instance in a private subnet that needs to make an API call to an AWS service (e.g., DynamoDB). Which option avoids sending traffic through a NAT Gateway and over the public internet?**

A. Use a VPC Gateway Endpoint for DynamoDB.

B. Assign an Elastic IP to the instance.

C. Route the traffic to the Virtual Private Gateway.

D. This is not possible; all traffic to AWS services from a private subnet must use a NAT Gateway.

---

## Security Groups and Network ACLs

**241. At what level does a Security Group operate?**

A. Subnet level

B. VPC level

C. Instance level (acting on the ENI)

D. Availability Zone level

**242. At what level does a Network ACL (NACL) operate?**

A. Instance level

B. Subnet level

C. VPC level

D. Region level

**243. Which of the following is STATEFUL?**

A. Security Group

B. Network ACL

C. Route Table

D. Internet Gateway

**244. Which of the following is STATELESS?**

A. Security Group

B. NAT Gateway

C. Network ACL

D. Application Load Balancer

**245. What does "stateful" mean in the context of a Security Group?**

A. It remembers the state of the EC2 instance (running/stopped).

B. If you allow an inbound request, the corresponding outbound response is automatically allowed, regardless of outbound rules.

C. You must define rules for both inbound and outbound traffic explicitly.

D. It can only have "allow" rules.

**246. What does "stateless" mean in the context of a Network ACL?**

A. It does not track connections, so return traffic must be explicitly allowed by a corresponding outbound or inbound rule.

B. It cannot be modified once created.

C. It only processes TCP traffic.

D. It automatically allows all return traffic.

**247. Which type of rules do Security Groups support?**

A. Allow rules only

B. Deny rules only

C. Both Allow and Deny rules

D. Rate-limiting rules

**248. Which type of rules do Network ACLs support?**

A. Allow rules only

B. Deny rules only

C. Both Allow and Deny rules

D. Redirect rules

**249. How are rules evaluated in a Security Group?**

A. In numerical order, from lowest to highest.

B. All rules are evaluated before a decision is made to allow traffic.

C. In numerical order, from highest to lowest.

D. The first matching rule is applied.

**250. How are rules evaluated in a Network ACL?**

A. All rules are evaluated before making a decision.

B. In numerical order, from lowest to highest, and the first matching rule is applied.

C. In random order.

D. Only "Allow" rules are evaluated first, then "Deny" rules.

**251. What is the default configuration of a custom (non-default) Security Group?**

A. Allows all inbound and outbound traffic.

B. Denies all inbound traffic and allows all outbound traffic.

C. Allows all inbound traffic and denies all outbound traffic.

D. Denies all inbound and outbound traffic.

**252. What is the default configuration of the default Security Group for a VPC?**

A. Denies all inbound, allows all outbound.

B. Allows all inbound from other instances in the same security group, and allows all outbound.

C. Allows all inbound and outbound traffic.

D. Denies all traffic.

**253. What is the default configuration of a default Network ACL (created with a new VPC)?**

A. Denies all inbound and outbound traffic.

B. Allows all inbound and outbound traffic.

C. Allows all inbound traffic, denies all outbound.

D. Denies all inbound traffic, allows all outbound.

**254. What is the last rule in every Network ACL, which cannot be modified?**

A. An implicit rule that allows all traffic.

B. An explicit rule numbered 32767 that allows all traffic.

C. An implicit rule (*) that denies any traffic not matched by a preceding rule.

D. An explicit rule numbered 100 that allows all traffic.

**255. You want to allow web traffic to your EC2 instance. You have an inbound Security Group rule allowing TCP port 80. Because Security Groups are stateful, what outbound rule is required for the web server to send responses back to users?**

A. An outbound rule allowing traffic on all ports (0-65535) to 0.0.0.0/0.

B. An outbound rule allowing traffic on TCP port 80 to 0.0.0.0/0.

C. No outbound rule is required for the response traffic, as it's part of an established connection.

D. An outbound rule allowing traffic on ephemeral ports (1024-65535) to 0.0.0.0/0.

**256. You want to allow web traffic to your EC2 instance. The subnet's NACL has an inbound rule allowing TCP port 80. To allow the web server's response to leave the subnet, what outbound NACL rule is required?**

A. No outbound rule is needed because NACLs are stateful.

B. An outbound rule allowing traffic on TCP port 80.

C. An outbound rule allowing traffic on the ephemeral port range (1024-65535), as this is where the client will be listening for the response.

D. An outbound rule allowing all traffic.

**257. Can a Security Group rule's source or destination be another Security Group ID?**

A. No, the source/destination must always be a CIDR block.

B. Yes, this allows instances associated with the source security group to communicate with instances in the destination security group.

C. Yes, but only within the same Availability Zone.

D. No, this feature was deprecated in favor of prefix lists.

**258. You need to block a specific malicious IP address from accessing any instance in your subnet. What is the most effective way to do this?**

A. Add a "deny" rule for the IP address to every security group in the subnet.

B. Add an inbound "deny" rule for the IP address to the Network ACL associated with the subnet.

C. Modify the route table to create a blackhole route for that IP address.

D. Launch a new instance and migrate your application.

**259. How many Security Groups can be associated with a single EC2 instance (ENI)?**

A. Exactly one.

B. Up to five by default.

C. Up to ten by default.

D. Unlimited.

**260. How many Network ACLs can be associated with a single subnet?**

A. Exactly one.

B. Up to five.

C. One for inbound, one for outbound.

D. As many as needed.

**261. An EC2 instance is associated with two security groups. SG-A allows SSH from your IP. SG-B allows HTTP from anywhere. What traffic is allowed to the instance?**

A. Only SSH, because it is more specific.

B. The union of the rules: both SSH from your IP and HTTP from anywhere are allowed.

C. Only traffic that matches the rules in both security groups.

D. Neither, as having two security groups creates a conflict.

**262. A subnet is associated with a custom NACL that has no rules defined. What is the effect on traffic?**

A. All traffic is allowed because there are no "deny" rules.

B. All traffic is denied because it will hit the implicit deny rule at the end.

C. The subnet reverts to using the default NACL.

D. Only traffic within the subnet is allowed.

**263. Which firewall layer acts first on traffic coming from the internet into an EC2 instance?**

A. The Security Group.

B. The Network ACL.

C. The host-based firewall on the EC2 instance.

D. The Route Table.

**264. Which firewall layer acts last on traffic going from an EC2 instance out to the internet?**

A. The Security Group.

B. The Network ACL.

C. The host-based firewall on the EC2 instance.

D. The Route Table.

**265. You have a web server (Instance A) and a database server (Instance B) in the same private subnet. You want to allow Instance A to connect to Instance B on the MySQL port (3306). What is the most secure and efficient way to configure this with Security Groups?**

A. In Instance B's security group, allow inbound TCP 3306 from the private IP address of Instance A.

B. In Instance B's security group, allow inbound TCP 3306 from the security group ID of Instance A.

C. In Instance B's security group, allow inbound TCP 3306 from the entire subnet CIDR.

D. In the subnet's NACL, allow TCP 3306 from the subnet's CIDR to itself.

**266. Why is referencing a security group ID as a source considered more secure and scalable than using an IP address or CIDR block?**

A. Because security group IDs are encrypted.

B. Because it automatically updates if the source instance's IP address changes or if new instances are added to the source group.

C. Because it results in lower latency.

D. Because IP addresses are not allowed as sources in security groups.

**267. A custom NACL is created. What is its initial state?**

A. It allows all traffic.

B. It denies all traffic (due to the implicit deny).

C. It has a single rule (100) that allows all traffic.

D. It cannot be used until at least one rule is added.

**268. You have an inbound NACL rule `100 ALLOW TCP 22 from 0.0.0.0/0` and another rule `200 DENY TCP 22 from 1.2.3.4/32`. If a request comes from IP 1.2.3.4, what happens?**

A. It is allowed, because the ALLOW rule has a lower number and is processed first.

B. It is denied, because the DENY rule is more specific.

C. It is denied, because DENY rules always take precedence.

D. It is allowed, because the ALLOW rule matches a broader range.

**269. Can you associate a security group with multiple EC2 instances?**

A. No, a security group is 1-to-1 with an instance.

B. Yes, a single security group can be applied to many instances.

C. Yes, but only if the instances are in the same subnet.

D. Yes, but only if the instances are of the same type.

**270. Can you change the security groups associated with an EC2 instance after it has been launched?**

A. No, you must terminate and relaunch the instance.

B. Yes, you can change the security groups for a running instance at any time.

C. Yes, but the instance must be stopped first.

D. Yes, but only via the AWS CLI, not the console.

**271. What is the recommended practice for NACL rule numbering?**

A. Use sequential numbers (1, 2, 3, 4...).

B. Use large gaps between rule numbers (e.g., 100, 200, 300) to allow for inserting new rules later.

C. Use random numbers to make it harder for attackers to guess the ruleset.

D. Start with high numbers and work down.

**272. An instance's security group allows inbound port 80. The subnet's NACL denies inbound port 80. Will the instance receive traffic on port 80?**

A. Yes, because the security group is the final firewall.

B. No, because the NACL evaluates traffic first and will deny it.

C. It depends on the outbound rules.

D. Yes, but only from within the same VPC.

**273. An instance's security group denies all traffic (hypothetically, if it supported deny). The subnet's NACL allows all traffic. Will the instance receive traffic?**

A. Yes, because the NACL allows it.

B. No, because the security group would block it.

C. Security groups don't support deny rules, so the premise is invalid. All traffic is denied by default unless explicitly allowed.

D. It depends on the route table.

**274. Which of the two, Security Groups or NACLs, can be used to control access between instances in the same subnet?**

A. Only Network ACLs.

B. Only Security Groups.

C. Both can be used for this purpose.

D. Neither, instances in the same subnet can always communicate.

**275. You are troubleshooting a "connection timed out" error when trying to SSH to an EC2 instance. Which is more likely to be the cause?**

A. A Network ACL rule denying the traffic.

B. A Security Group rule that does not allow the traffic.

C. A route table issue.

D. A DHCP options set misconfiguration.

**276. You are troubleshooting a "connection refused" error when trying to connect to a service on an EC2 instance. What does this typically indicate?**

A. A Security Group or NACL is blocking the traffic.

B. The network path is correct, but no process is listening on the destination port on the instance.

C. The route table has a blackhole route.

D. The Internet Gateway is detached.

**277. A subnet can be associated with a custom NACL. If you disassociate it, what happens?**

A. The subnet has no NACL and all traffic is allowed.

B. The subnet automatically re-associates with the VPC's default NACL.

C. All traffic to and from the subnet is blocked.

D. You cannot disassociate a NACL from a subnet.

**278. Security Groups are considered the first line of defense at the _____ level.**

A. Subnet

B. VPC

C. Instance

D. Region

**279. Network ACLs are considered the first line of defense at the _____ level.**

A. Subnet

B. VPC

C. Instance

D. Availability Zone

**280. You have a three-tier application (web, app, db). What is the best practice for structuring security groups?**

A. Use one large security group for all three tiers.

B. Create a separate security group for each tier (e.g., web-sg, app-sg, db-sg) and reference them as sources in the rules.

C. Use only Network ACLs to control traffic between tiers.

D. Place all tiers in the same security group but in different subnets.

**281. Can you delete the default security group of a VPC?**

A. Yes, at any time.

B. No, you cannot delete the default security group.

C. Yes, but only if no resources are using it.

D. Yes, but you must create a new one to replace it first.

**282. Can you delete the default Network ACL of a VPC?**

A. Yes, at any time.

B. No, you cannot delete the default Network ACL.

C. Yes, but only if no subnets are associated with it.

D. Yes, but you must create a new one to replace it first.

**283. A security group rule allows inbound traffic from source `sg-12345`. This means...**

A. Any traffic from the internet is allowed.

B. Any resource associated with security group `sg-12345` can send traffic to the instance.

C. Only traffic from the instance with ID `i-12345` is allowed.

D. Traffic from the subnet where `sg-12345` is located is allowed.

**284. What is the ephemeral port range that you need to consider for NACL outbound rules?**

A. 0-1023

B. 80-443

C. 1024-65535

D. Only port 22

**285. If you modify a rule in a security group, how quickly does the change take effect?**

A. After a 5-minute propagation delay.

B. Instantly or within a few seconds.

C. After you reboot the associated instances.

D. During the next maintenance window.

**286. Which of the following is a key difference between Security Groups and NACLs?**

A. SGs are stateless, NACLs are stateful.

B. SGs support allow rules only, NACLs support allow and deny rules.

C. SGs operate at the subnet level, NACLs at the instance level.

D. SGs process rules in numerical order, NACLs evaluate all rules.

**287. You have an EC2 instance that can't reach the internet. You've confirmed the route table and public IP are correct. The security group has the default outbound rule (Allow All). What should you check next?**

A. The security group's inbound rules.

B. The subnet's Network ACL for an outbound rule that might be blocking the traffic.

C. The VPC's DHCP options set.

D. The instance's IAM role.

**288. Can a Network ACL rule's source or destination be a Security Group ID?**

A. Yes, this is a common practice.

B. No, NACL rules must use CIDR blocks.

C. Yes, but only for the default NACL.

D. Only for outbound rules.

**289. By default, how many inbound and outbound rules can you have per security group?**

A. 10

B. 25

C. 60

D. 100

**290. By default, how many rules can you have per Network ACL (in each direction)?**

A. 20

B. 50

C. 100

D. 40 (20 inbound, 20 outbound)

**291. You have a fleet of web servers behind an Elastic Load Balancer. What should the source of the inbound HTTP/HTTPS rule be on the web servers' security group?**

A. 0.0.0.0/0

B. The CIDR block of the subnet containing the ELB.

C. The security group of the Elastic Load Balancer.

D. The public IP addresses of the ELB nodes.

**292. Security groups are associated with _____, while Network ACLs are associated with _____.**

A. Subnets, Instances

B. Instances/ENIs, Subnets

C. VPCs, Subnets

D. Route Tables, Instances

**293. If you want to create a "demilitarized zone" (DMZ) in your VPC, which tool would you primarily use to create the boundary?**

A. Security Groups

B. Subnets and Network ACLs

C. Route Tables

D. VPC Peering

**294. The default NACL allows all traffic. A custom NACL denies all traffic by default. Why the difference?**

A. The default NACL is designed for ease of use and to not break connectivity unexpectedly. Custom NACLs assume a "deny by default" security posture.

B. This is incorrect; both allow all traffic by default.

C. This is incorrect; both deny all traffic by default.

D. The default NACL is stateful, while custom NACLs are stateless.

**295. Can security groups span across different VPCs?**

A. Yes, if the VPCs are peered.

B. Yes, security groups are a regional resource.

C. No, a security group is tied to a specific VPC.

D. No, unless using a Transit Gateway.

**296. You can reference a security group in a different VPC (in a different region) as a source in your security group rules if you have an inter-region VPC peering connection.**

A. True

B. False. You must use the CIDR block of the peered VPC.

C. True, but only for TCP traffic.

D. False, inter-region peering does not support this.

**297. Which of the following provides a more granular level of control?**

A. Network ACLs, because they can deny traffic.

B. Security Groups, because they can be applied per-instance/ENI.

C. Route Tables, because they control the path of traffic.

D. They provide the same level of granularity.

**298. An EC2 instance has a security group that allows inbound TCP port 22 from 10.0.0.5/32. The subnet NACL has a rule `100 DENY ALL traffic from 10.0.0.0/16` and a rule `200 ALLOW ALL traffic from 0.0.0.0/0`. What happens to an SSH attempt from 10.0.0.5?**

A. It is allowed because of the security group rule.

B. It is denied because the NACL rule 100 is processed first and matches.

C. It is allowed because of the NACL rule 200.

D. It is denied because the security group does not have an outbound rule.

**299. When troubleshooting, it's important to remember the order of operations for inbound traffic:**

A. Security Group -> Network ACL -> Route Table

B. Route Table -> Network ACL -> Security Group -> Instance Firewall

C. Network ACL -> Security Group -> Route Table -> Instance Firewall

D. Route Table -> Security Group -> Network ACL -> Instance Firewall

**300. You have a web server that needs to make an outbound connection to an external API on port 443. The server's security group has the default outbound rule (Allow All). The subnet's NACL has a default configuration (Allow All). Will the connection work?**

A. No, you need to explicitly allow outbound port 443 in the security group.

B. No, you need to explicitly allow outbound port 443 in the NACL.

C. Yes, the default rules for both SG and NACL are sufficient to allow this outbound connection.

D. It depends on the inbound rules.

**301. You want to prevent your developers from accidentally launching instances that are open to the world on SSH (port 22). What is a good preventative measure?**

A. Create a custom NACL for all subnets that has a DENY rule for port 22 from 0.0.0.0/0.

B. Modify the default security group to remove the allow-all rule from itself.

C. Use AWS Config to detect and alert on security groups with inbound 0.0.0.0/0 on port 22.

D. All of the above are valid strategies.

**302. Can a single ENI be associated with security groups from different VPCs?**

A. Yes, if the VPCs are peered.

B. No, an ENI and its associated security groups must all belong to the same VPC.

C. Yes, this is a standard feature.

D. Only if using AWS Transit Gateway.

**303. What is the source for the default inbound rule in a VPC's default security group?**

A. 0.0.0.0/0

B. The VPC's CIDR block.

C. The ID of the default security group itself.

D. There are no default inbound rules.

**304. Why would you need an outbound NACL rule for ephemeral ports (1024-65535)?**

A. To allow instances to initiate outbound connections.

B. To allow responses to inbound requests to leave the subnet.

C. This is not necessary as NACLs are stateful.

D. To allow traffic between instances in the same subnet.

**305. If you have a very strict NACL, can it block traffic between two instances in the same subnet?**

A. No, traffic within a subnet does not pass through the NACL.

B. Yes, all traffic entering or leaving the subnet boundary is checked by the NACL, even if the destination is in the same subnet.

C. Only if the instances are in different security groups.

D. This is incorrect. Traffic between instances in the same subnet does not leave the subnet, so the NACL is not applied.

**306. Which firewall is better suited for fine-grained access control, like allowing one specific EC2 instance to talk to another?**

A. Network ACLs, because they have deny rules.

B. Security Groups, because they operate at the instance level and can reference other groups.

C. Both are equally suited.

D. Route Tables.

**307. You have an inbound NACL rule `100 ALLOW TCP 80` and an outbound rule `100 ALLOW TCP 80`. A client connects to your web server. Will the response get back to the client?**

A. Yes, because outbound TCP 80 is allowed.

B. No, because the response will be on an ephemeral port, which is not allowed by the outbound rule.

C. Yes, because NACLs are stateful.

D. It depends on the security group.

**308. Can you add a description to a security group rule?**

A. No, descriptions are not supported.

B. Yes, and it is a best practice for documenting the purpose of the rule.

C. Only via the AWS CLI.

D. Only for inbound rules.

**309. What is the maximum number of security groups you can create per VPC by default?**

A. 100

B. 500

C. 2500

D. 10000

**310. What is the maximum number of Network ACLs you can create per VPC by default?**

A. 50

B. 100

C. 200

D. 500

**311. A security group is a virtual firewall for your instance to control inbound and outbound traffic. What is the equivalent for a subnet?**

A. Another Security Group

B. A Route Table

C. A Network ACL

D. An Internet Gateway

**312. If you remove all rules from a security group, what is the effect?**

A. All traffic is allowed.

B. All traffic is denied.

C. Only outbound traffic is allowed.

D. The security group is deleted.

**313. You have a rule in your NACL: `Rule #100, Type: ALL Traffic, Protocol: ALL, Port Range: ALL, Source: 0.0.0.0/0, Allow/Deny: DENY`. What is the effect of this rule?**

A. It has no effect because of the implicit deny rule.

B. It blocks all inbound traffic to the subnet.

C. It blocks all outbound traffic from the subnet.

D. It depends if it's in the inbound or outbound list, but it will block all traffic in that direction.

**314. Can you use DNS names (e.g., google.com) as a source or destination in a security group rule?**

A. Yes, this is a new feature.

B. No, you must use CIDR blocks, prefix lists, or other security group IDs.

C. Yes, but only for outbound rules.

D. Only if you enable DNS support for the VPC.

**315. Which of the following is a key operational difference between managing Security Groups and NACLs?**

A. SG changes take hours to apply, NACL changes are instant.

B. SGs are applied to instances, so you might manage many SGs. NACLs are applied to subnets, so you typically manage fewer NACLs.

C. SGs are managed via IAM, NACLs are managed via the EC2 console.

D. There are no significant operational differences.

**316. The default security group for a VPC initially allows:**

A. All inbound traffic from the internet.

B. All inbound traffic from other members of the same security group.

C. No inbound traffic.

D. Inbound SSH and HTTP traffic from anywhere.

**317. If you want to quickly block a large list of known bad IP ranges, which is the better tool?**

A. Security Groups, because they are stateful.

B. Network ACLs, because they support explicit deny rules and are processed before SGs.

C. AWS WAF.

D. Route table blackholing.

**318. An instance is launched without specifying a security group. What happens?**

A. The launch fails.

B. It is launched with no security group, allowing all traffic.

C. It is automatically assigned the default security group for the VPC.

D. A new, empty security group is created for it.

**319. A subnet is created without specifying a Network ACL. What happens?**

A. The creation fails.

B. It is launched with no NACL, allowing all traffic.

C. It is automatically associated with the default Network ACL for the VPC.

D. A new, custom NACL that denies all traffic is created for it.

**320. Which statement is true about the relationship between Security Groups and Network ACLs?**

A. They are mutually exclusive; you can use one or the other, but not both.

B. They work together as layered security controls; traffic must be allowed by both to reach an instance.

C. Security Groups override Network ACLs.

D. Network ACLs override Security Groups.

**321. You have a security group rule that allows traffic from a specific prefix list. What is a prefix list?**

A. A list of security group IDs.

B. A customer-managed set of one or more CIDR blocks.

C. A list of IAM users.

D. A list of domain names.

**322. Why might you use a prefix list in a security group instead of listing CIDR blocks directly?**

A. It's cheaper.

B. It allows you to group and reuse sets of CIDR blocks, simplifying rule management across multiple security groups.

C. Prefix lists support DNS names.

D. It's the only way to specify more than one CIDR block.

**323. A security group rule can specify a protocol. If you select 'All traffic', what does this cover?**

A. Only TCP and UDP.

B. Only TCP, UDP, and ICMP.

C. All IP protocols.

D. Only HTTP and HTTPS.

**324. A NACL rule is set for protocol 'ICMP'. What is this commonly used for?**

A. Web traffic.

B. File transfers.

C. Network diagnostics like 'ping'.

D. Remote desktop connections.

**325. You are unable to ping an instance in a public subnet from your laptop. You have confirmed the security group allows all ICMP traffic. What is a likely NACL issue?**

A. The inbound NACL rule allows ICMP, but the outbound NACL rule does not allow the ICMP echo reply.

B. The NACL does not support ICMP.

C. The outbound NACL rule is blocking your laptop's IP.

D. The inbound NACL rule is blocking port 80.

**326. Can you modify the rules of the default security group?**

A. No, it is read-only.

B. Yes, you can add or remove rules from it just like any other security group.

C. You can only add rules, not remove the default ones.

D. You can only remove rules, not add new ones.

**327. Can you modify the rules of the default Network ACL?**

A. No, it is read-only.

B. Yes, you can add or remove rules from it just like any other NACL.

C. You can only add rules, not remove the default ones.

D. You can only remove rules, not add new ones.

**328. Which of these acts as a firewall at the instance level?**

A. Network ACL

B. Route Table

C. Security Group

D. Internet Gateway

**329. Which of these acts as a firewall at the subnet level?**

A. Network ACL

B. Route Table

C. Security Group

D. Virtual Private Gateway

**330. To allow an RDS database instance to be accessed by a fleet of EC2 application servers, the most secure method is to:**

A. Place the RDS instance in a public subnet.

B. In the RDS instance's security group, add an inbound rule allowing the database port from the security group of the application servers.

C. In the RDS instance's security group, add an inbound rule allowing the database port from 0.0.0.0/0.

D. In the subnet's NACL, allow all traffic.

**331. You have a security group with no inbound rules and the default outbound rule. An instance in this group tries to ping 8.8.8.8. What happens?**

A. The ping fails because the outbound rule is processed first.

B. The ping fails because the ICMP echo reply will be blocked by the lack of an inbound rule.

C. The ping succeeds because security groups are stateful and the outbound request is allowed, so the reply is automatically allowed.

D. The ping succeeds because ICMP is always allowed.

**332. You have a NACL with an inbound rule allowing all traffic and an outbound rule denying all traffic. An instance in the associated subnet tries to ping 8.8.8.8. What happens?**

A. The ping succeeds because the inbound rule allows the reply.

B. The ping fails because the outbound ICMP echo request is denied before it can leave the subnet.

C. The ping succeeds because NACLs are stateful.

D. The ping fails because the security group will block it.

**333. Security groups are a regional resource, but they are scoped to a specific...**

A. Availability Zone

B. Subnet

C. VPC

D. AWS Account

**334. You have two instances in the same subnet and the same security group. The security group has no rules. Can they communicate?**

A. Yes, instances in the same security group can always communicate.

B. No, because there are no rules allowing traffic, even from the same group.

C. Yes, because they are in the same subnet.

D. It depends on the Network ACL.

**335. You have two instances in the same subnet and the same security group. The default security group rule (allow all traffic from the group itself) is present. Can they communicate?**

A. No, you still need to add rules for specific ports.

B. Yes, the default rule allows them to communicate freely.

C. No, because they are in the same subnet, they bypass the security group.

D. Only if the NACL also allows it.

**336. Which component is NOT part of the VPC security layers?**

A. Security Groups

B. Network ACLs

C. Route Tables

D. DHCP Options Sets

**337. If you need to troubleshoot network connectivity to an instance, which AWS service can provide detailed logs about accepted and rejected traffic at the ENI level?**

A. AWS CloudTrail

B. VPC Flow Logs

C. Amazon CloudWatch Metrics

D. AWS X-Ray

**338. A NACL rule number must be between:**

A. 1 and 100

B. 1 and 32766

C. 100 and 1000

D. 0 and 255

**339. What is the number of the final, implicit deny rule in a NACL?**

A. 32767

B. * (asterisk)

C. 99999

D. There is no implicit deny.

**340. For an Application Load Balancer to be able to perform health checks on its target instances, what traffic must the instances' security group allow?**

A. All traffic from 0.0.0.0/0.

B. Traffic on the health check port from the security group of the load balancer.

C. ICMP traffic from the load balancer's private IPs.

D. All traffic from the subnet where the load balancer resides.

## Elastic IP

**341. What is an Elastic IP (EIP) address?**

A. A dynamic public IPv4 address that changes every time an instance reboots.

B. A static, public IPv4 address designed for dynamic cloud computing.

C. A private IP address that can be moved between instances.

D. A static IPv6 address.

**342. What is the primary use case for an Elastic IP address?**

A. To give an instance a predictable, public-facing IP address that can be remapped to a new instance in case of failure.

B. To enable communication between instances in a private subnet.

C. To reduce data transfer costs.

D. To provide DNS resolution.

**343. Under what condition are you charged for an Elastic IP address?**

A. When it is allocated to your account.

B. When it is associated with a running EC2 instance.

C. When it is allocated to your account but NOT associated with a running instance, or when it's associated with a stopped instance.

D. Elastic IPs are always free of charge.

**344. What happens to a standard auto-assigned public IP address when you stop an EC2 instance?**

A. It remains associated with the instance.

B. It is released, and you get a new one when you start the instance again.

C. It is converted into an Elastic IP.

D. The instance is terminated.

**345. What happens to an Elastic IP address when you stop the EC2 instance it is associated with?**

A. It is released from your account.

B. It remains associated with the stopped instance.

C. It becomes disassociated from the instance but remains in your account.

D. It is assigned to another running instance automatically.

**346. Can you associate an Elastic IP address with an EC2 instance in a private subnet?**

A. No, instances in private subnets cannot have public IPs.

B. Yes, but it will not provide internet connectivity without a proper route table entry to an IGW.

C. Yes, and it automatically makes the subnet public.

D. No, Elastic IPs can only be associated with NAT Gateways.

**347. Besides an EC2 instance, what other AWS resource is commonly associated with an Elastic IP address?**

A. An S3 Bucket

B. A Security Group

C. A NAT Gateway

D. An IAM User

**348. How do you release an Elastic IP address that you no longer need?**

A. It is released automatically after 24 hours of non-use.

B. You must explicitly release it from the EC2 or VPC console.

C. You must disassociate it from any resource, and then it is automatically released.

D. You must open a support ticket.

**349. What is the default limit on the number of Elastic IPs you can have in your account per region?**

A. 1

B. 5

C. 20

D. 50

**350. When you associate an Elastic IP with an EC2 instance that already has an auto-assigned public IP, what happens?**

A. The association fails.

B. The auto-assigned public IP is released, and the Elastic IP takes its place.

C. The instance now has two public IP addresses.

D. The instance must be rebooted for the change to take effect.

**351. Can an Elastic IP address be moved from an instance in one Availability Zone to an instance in another Availability Zone?**

A. No, an EIP is tied to a specific AZ.

B. Yes, as long as both instances are in the same region.

C. Yes, but only if the instances are in the same VPC.

D. No, an EIP can only be moved between instances in the same subnet.

**352. Can an Elastic IP address be moved from an instance in the us-east-1 region to an instance in the us-west-2 region?**

A. Yes, EIPs are global resources.

B. No, an EIP is specific to the region in which it was allocated.

C. Yes, if you use AWS Transit Gateway.

D. Yes, but it incurs a data transfer fee.

**353. An Elastic IP address is associated with which underlying component?**

A. The EC2 instance ID.

B. The subnet ID.

C. The Elastic Network Interface (ENI).

D. The security group.

**354. Why does AWS charge for unassociated Elastic IPs?**

A. To cover the cost of the IP address itself.

B. To encourage efficient use of a limited public IPv4 address space.

C. Because they consume more network resources when unassociated.

D. This is a billing error; they are supposed to be free.

**355. You have a web server that needs a static, public IP address for DNS 'A' record pointing. Which IP type should you use?**

A. An auto-assigned public IP.

B. A private IP.

C. An Elastic IP.

D. An IPv6 address.

**356. If you terminate an EC2 instance that has an Elastic IP associated with it, what happens to the EIP?**

A. The EIP is also terminated.

B. The EIP is disassociated and remains in your account.

C. The EIP is released back to AWS's pool.

D. The EIP is transferred to the default VPC.

**357. Elastic IPs are for which IP version?**

A. IPv4 only

B. IPv6 only

C. Both IPv4 and IPv6

D. They are version-agnostic.

**358. To associate an EIP with an instance, the instance must be in what state?**

A. Stopped

B. Terminated

C. Running or stopped

D. Pending

**359. What is the "Bring Your Own IP" (BYOIP) feature?**

A. It allows you to use your own private IP addresses in a VPC.

B. It allows you to bring a range of public IPv4 addresses that you own to AWS and use them as Elastic IPs.

C. It's a way to purchase vanity IP addresses.

D. It allows you to use IPv6 addresses as EIPs.

**360. Can a single EC2 instance have multiple Elastic IP addresses associated with it?**

A. No, an instance can only have one public IP.

B. Yes, by associating EIPs with multiple Elastic Network Interfaces (ENIs) attached to the instance.

C. Yes, you can attach multiple EIPs to the primary ENI.

D. No, this is not a supported configuration.

**361. When you allocate an Elastic IP, you are allocating it from which pool?**

A. A global pool of IP addresses.

B. Amazon's pool of public IPv4 addresses for that specific region.

C. Your VPC's CIDR range.

D. A pool shared with your on-premises network.

**362. You have an EIP associated with a running instance. Is there a charge for this EIP?**

A. Yes, all EIPs have an hourly charge.

B. No, the first EIP associated with a running instance is free of charge.

C. Yes, but only for the data transferred through it.

D. No, EIPs are always free.

**363. What is the process of moving an EIP from a failed instance to a standby instance called?**

A. IP Re-routing

B. IP Failover

C. IP Remapping or Reassociation

D. IP Hot-swapping

**364. An Elastic IP provides an instance with a static public IP. Does it also provide internet access?**

A. Yes, automatically.

B. No, internet access also requires the VPC to have an Internet Gateway and a route table entry pointing to it.

C. Yes, but only for outbound traffic.

D. No, it only provides a static private IP.

**365. Can you associate an Elastic IP with an Application Load Balancer?**

A. Yes, this is how you get a static IP for an ALB.

B. No, ALBs do not have static IPs. You should use a Network Load Balancer if you need a static IP for a load balancer.

C. Yes, but only for internet-facing ALBs.

D. No, EIPs are only for EC2 instances.

**366. A Network Load Balancer can be assigned an Elastic IP for each subnet it is enabled in.**

A. True

B. False

C. Only for internal NLBs

D. Only for TCP listeners

**367. When you disassociate an EIP from an ENI, the ENI's public IP address is...**

A. Unchanged.

B. Released, if it was an auto-assigned public IP.

C. Set to 0.0.0.0.

D. Converted to a private IP.

**368. The main benefit of an EIP over a standard public IP is that the EIP is _____ to your AWS account.**

A. Tied

B. Billed

C. Limited

D. Released

**369. If you have an EIP associated with a NAT Gateway, are you charged for the EIP?**

A. Yes, there is always a charge for EIPs on NAT Gateways.

B. No, an EIP associated with a used NAT Gateway is not charged, similar to an EIP on a running instance.

C. Yes, but at a reduced rate.

D. Only if the NAT Gateway is idle.

**370. To mask the failure of an instance or software by rapidly remapping a public IP address to another instance in your account, you should use:**

A. A DNS CNAME record.

B. An Elastic IP address.

C. A NAT Gateway.

D. VPC Peering.

## DHCP Options Set

**371. What is the purpose of a DHCP Options Set in a VPC?**

A. To assign static IP addresses to EC2 instances.

B. To provide a set of network configuration parameters (like domain name, DNS servers, NTP servers) to instances in a VPC.

C. To control routing between subnets.

D. To filter inbound and outbound traffic.

**372. Which of the following is a configurable parameter in a DHCP Options Set?**

A. IP address range for the subnet.

B. Domain name servers.

C. Security group ID.

D. Route table ID.

**373. When you create a VPC, what DHCP options set is it associated with by default?**

A. No DHCP options set.

B. A default DHCP options set created by AWS.

C. A custom DHCP options set that you must create first.

D. An empty DHCP options set.

**374. What is the default DNS server specified in the default DHCP Options Set?**

A. 8.8.8.8 (Google DNS)

B. The Amazon-provided DNS server (at the .2 address of the VPC's CIDR).

C. 1.1.1.1 (Cloudflare DNS)

D. No DNS server is specified by default.

**375. How many DHCP Options Sets can be associated with a VPC at one time?**

A. One per subnet.

B. One per Availability Zone.

C. Exactly one.

D. Up to five.

**376. If you want your EC2 instances in a VPC to use your on-premises DNS servers for name resolution, what should you do?**

A. Manually configure the DNS settings on each EC2 instance.

B. Create a new DHCP Options Set specifying your on-premises DNS servers and associate it with the VPC.

C. Modify the route table to point to your DNS servers.

D. This is not possible; you must use the Amazon DNS server.

**377. Which of the following is NOT a configurable option in a DHCP Options Set?**

A. Domain name

B. NTP servers

C. NetBIOS name servers

D. Default Gateway

**378. After you create a DHCP options set, you can modify it.**

A. True, you can edit all options at any time.

B. False, DHCP options sets are immutable. To change it, you must create a new one and associate it with the VPC.

C. True, but only the domain name can be changed.

D. False, unless no VPC is associated with it.

**379. What is the purpose of the `domain-name` option in a DHCP Options Set?**

A. It sets the public domain name for the VPC.

B. It provides a default domain name for instances to use when resolving hostnames.

C. It registers the VPC with a domain registrar.

D. It is used for VPC peering.

**380. If you associate a new DHCP options set with a VPC, when do existing instances pick up the changes?**

A. Immediately.

B. After a few minutes.

C. When their DHCP lease is renewed, or when they are rebooted.

D. They do not pick up the changes; only new instances will use the new set.

**381. You want your instances to synchronize their time with your corporate NTP servers. Where do you configure this for the entire VPC?**

A. In the Security Group.

B. In the Route Table.

C. In a custom DHCP Options Set.

D. In the instance user data.

**382. Can you delete a DHCP options set?**

A. No, they cannot be deleted.

B. Yes, but only if it is not associated with any VPC.

C. Yes, at any time. Deleting it will cause associated VPCs to revert to the default set.

D. No, you can only disassociate it.

**383. The Amazon DNS server is also referred to as:**

A. Route 53

B. The .1 address in the subnet

C. The AmazonProvidedDNS or the .2 address of the VPC CIDR

D. The .254 address in the subnet

**384. If you specify "AmazonProvidedDNS" as the DNS server in your custom DHCP options set, what does it resolve to?**

A. 8.8.8.8

B. The IP address of the Amazon DNS server for your VPC.

C. Your on-premises DNS server.

D. It resolves to nothing; it's just a placeholder.

**385. You have a hybrid environment with AWS Direct Connect. To allow instances in your VPC to resolve hostnames in your on-premises network, you should configure the DHCP Options Set to point to:**

A. The Amazon DNS server.

B. Your on-premises DNS servers.

C. The Virtual Private Gateway IP address.

D. A Route 53 Resolver endpoint.

**386. A DHCP Options Set is a _____ resource.**

A. Global

B. Regional

C. Zonal

D. VPC-specific

**387. What happens if you delete a VPC?**

A. The associated DHCP options set is also deleted.

B. The DHCP options set is disassociated but remains in your account.

C. The DHCP options set is moved to the default VPC.

D. You cannot delete a VPC with a custom DHCP options set.

**388. Which of the following options is related to Windows instances and can be configured in a DHCP Options Set?**

A. NTP servers

B. NetBIOS node type

C. DNS servers

D. Domain name

**389. If you set custom DNS servers in your DHCP options set, what is a potential side effect?**

A. You will be charged more for DNS queries.

B. Instances may no longer be able to resolve the private DNS hostnames of other instances in the VPC.

C. Network performance will decrease.

D. Security groups will stop working.

**390. To use both your on-premises DNS servers and the Amazon DNS server, what service should you use in conjunction with your DHCP options set?**

A. Amazon Route 53 Private Hosted Zones

B. Amazon Route 53 Resolver (with forwarding rules)

C. VPC Peering

D. AWS Transit Gateway

**391. The DHCP options set provides configuration to the _____ on an EC2 instance.**

A. IAM Role

B. Operating System's network configuration

C. Security Group

D. EBS Volume

**392. Can you have a VPC with no DHCP options set associated with it?**

A. Yes, if you manually configure networking on all instances.

B. No, every VPC must have one and only one DHCP options set associated with it.

C. Yes, this is the default for custom VPCs.

D. Only if the VPC has no subnets.

**393. The default DHCP options set created by AWS for your account can be deleted.**

A. True

B. False

C. Only if it's not associated with any VPC.

D. Only by contacting AWS Support.

**394. If you change the DHCP options set for a VPC, what is the most reliable way to ensure a Linux instance gets the new settings?**

A. Wait for 5 minutes.

B. Run `sudo dhclient -r && sudo dhclient`.

C. Reboot the instance.

D. Modify the security group.

**395. The primary role of DHCP in a VPC is to provide instances with their:**

A. Public IP address.

B. Private IP address and other network configuration options.

C. Security group rules.

D. IAM credentials.

**396. You want all instances in your VPC to have the domain suffix `corp.example.com`. Where do you configure this?**

A. In the VPC settings.

B. In a custom DHCP Options Set under the `domain-name` option.

C. In the Route 53 private hosted zone.

D. In the user data of each instance.

**397. If you specify four DNS servers in your DHCP options set, how are they provided to the client OS?**

A. Only the first one is used.

B. They are provided as an ordered list.

C. They are load-balanced.

D. The client randomly picks one.

**398. Is there a direct cost associated with creating or using DHCP Options Sets?**

A. Yes, there is a per-hour charge.

B. Yes, you are charged per option configured.

C. No, there is no additional charge for DHCP options sets.

D. No, but using custom DNS servers may incur costs on those servers.

**399. The DHCP options set is crucial for integrating a VPC with:**

A. An S3 bucket.

B. A hybrid network environment (e.g., on-premises DNS).

C. An Elastic Load Balancer.

D. AWS WAF.

**400. If you disassociate a custom DHCP options set from a VPC, what happens?**

A. The VPC has no DHCP settings.

B. The VPC automatically associates with the default DHCP options set.

C. The VPC keeps a cached copy of the custom settings.

D. All instances in the VPC lose network connectivity.

---

## Answer Key

| | | | | |
|---|---|---|---|---|
| 1: B | 2: C | 3: A | 4: A | 5: B |
| 6: C | 7: B | 8: B | 9: A | 10: B |
| 11: B | 12: B | 13: B | 14: A | 15: B |
| 16: B | 17: B | 18: C | 19: C | 20: D |
| 21: A | 22: B | 23: B | 24: C | 25: B |

| | | | | |
|---|---|---|---|---|
| 26: C | 27: C | 28: C | 29: B | 30: C |
| 31: C | 32: B | 33: D | 34: A | 35: B |
| 36: C | 37: B | 38: B | 39: C | 40: B |
| 41: B | 42: B | 43: C | 44: B | 45: A |
| 46: A | 47: C | 48: A | 49: C | 50: B |
| 51: B | 52: B | 53: B | 54: D | 55: C |
| 56: A | 57: D | 58: B | 59: B | 60: B |
| 61: C | 62: C | 63: B | 64: C | 65: B |
| 66: B | 67: D | 68: B | 69: C | 70: B |
| 71: C | 72: C | 73: C | 74: D | 75: D |
| 76: B | 77: B | 78: B | 79: C | 80: B |
| 81: B | 82: B | 83: C | 84: B | 85: B |
| 86: B | 87: C | 88: C | 89: C | 90: B |
| 91: C | 92: B | 93: B | 94: C | 95: B |
| 96: A | 97: C | 98: C | 99: B | 100: B |
| 101: B | 102: C | 103: B | 104: C | 105: B |
| 106: C | 107: C | 108: B | 109: C | 110: C |
| 111: B | 112: B | 113: B | 114: B | 115: C |
| 116: B | 117: A | 118: C | 119: B | 120: B |

| | | | | |
|---|---|---|---|---|
| 121: B | 122: C | 123: A | 124: B | 125: C |
| 126: B | 127: A | 128: C | 129: B | 130: B |
| 131: B | 132: B | 133: A | 134: B | 135: B |
| 136: C | 137: B | 138: C | 139: C | 140: B |
| 141: B | 142: A | 143: A | 144: C | 145: C |
| 146: A | 147: C | 148: B | 149: C | 150: A |
| 151: A | 152: C | 153: A | 154: B | 155: B |
| 156: C | 157: B | 158: B | 159: B | 160: A |
| 161: C | 162: B | 163: A | 164: D | 165: C |
| 166: B | 167: B | 168: B | 169: B | 170: A |
| 171: C | 172: C | 173: B | 174: A | 175: B |
| 176: A | 177: A | 178: B | 179: B | 180: A |
| 181: B | 182: B | 183: B | 184: A | 185: A |
| 186: C | 187: A | 188: B | 189: B | 190: C |
| 191: A | 192: C | 193: B | 194: B | 195: B |
| 196: B | 197: D | 198: C | 199: B | 200: B |
| 201: B | 202: B | 203: A | 204: B | 205: A |
| 206: B | 207: B | 208: C | 209: B | 210: B |
| 211: B | 212: B | 213: B | 214: B | 215: C |

| | | | | |
|---|---|---|---|---|
| 216: B | 217: D | 218: A | 219: B | 220: B |
| 221: B | 222: B | 223: A | 224: D | 225: C |
| 226: B | 227: B | 228: B | 229: C | 230: B |
| 231: A | 232: B | 233: A | 234: B | 235: B |
| 236: A | 237: B | 238: A | 239: B | 240: A |
| 241: C | 242: B | 243: A | 244: C | 245: B |
| 246: A | 247: A | 248: C | 249: B | 250: B |
| 251: B | 252: B | 253: B | 254: C | 255: C |
| 256: C | 257: B | 258: B | 259: B | 260: A |
| 261: B | 262: B | 263: B | 264: B | 265: B |
| 266: B | 267: B | 268: A | 269: B | 270: B |
| 271: B | 272: B | 273: C | 274: C | 275: B |
| 276: B | 277: B | 278: C | 279: A | 280: B |
| 281: B | 282: B | 283: B | 284: C | 285: B |
| 286: B | 287: B | 288: B | 289: C | 290: A |
| 291: C | 292: B | 293: B | 294: A | 295: C |
| 296: B | 297: B | 298: B | 299: B | 300: C |
| 301: D | 302: B | 303: C | 304: B | 305: D |
| 306: B | 307: B | 308: B | 309: C | 310: C |

| | | | | |
|---|---|---|---|---|
| 311: C | 312: B | 313: D | 314: B | 315: B |
| 316: B | 317: B | 318: C | 319: C | 320: B |
| 321: B | 322: B | 323: C | 324: C | 325: A |
| 326: B | 327: B | 328: C | 329: A | 330: B |
| 331: C | 332: B | 333: C | 334: B | 335: B |
| 336: D | 337: B | 338: B | 339: B | 340: B |
| 341: B | 342: A | 343: C | 344: B | 345: B |
| 346: B | 347: C | 348: B | 349: B | 350: B |
| 351: B | 352: B | 353: C | 354: B | 355: C |
| 356: B | 357: A | 358: C | 359: B | 360: B |
| 361: B | 362: B | 363: C | 364: B | 365: B |
| 366: A | 367: B | 368: A | 369: B | 370: B |
| 371: B | 372: B | 373: B | 374: B | 375: C |
| 376: B | 377: D | 378: B | 379: B | 380: C |
| 381: C | 382: B | 383: C | 384: B | 385: B |
| 386: B | 387: B | 388: B | 389: B | 390: B |
| 391: B | 392: B | 393: B | 394: C | 395: B |
| 396: B | 397: B | 398: C | 399: B | 400: B |