**VPC**:

>>> VPC stands for Virtual Private Cloud.

>>> VPC allows you to easily customize your networking configuration.

>>> VPC is a network that is logically isolated from other network in the cloud.

>>> It allows you to have your own IP address range, subnets, internet gateways, NAT gateways and security groups.

**IP address**:

>>> IP stands for "Internet Protocol" address.

>>> An IP address is a unique string of numbers separated by periods (IPv4) or colons (IPv6) that identifies each computer using the Internet Protocol to communicate over a network.

Here's a simple way to understand it:

Example: Think of an IP address like a home address. Just as a home address identifies where you live, an IP address identifies a device on a network.

**IPv4**:

>>> IPv4 addresses are 32 bits length

>>> IPv4 uses decimal notation separated by dots

>>> IPv4 address can be divided into four sections and each section range from 0 to 255

>>> IPv4 can support around 4.3 billion unique addresses.

>>> IPv4 has less security features

Example: 192.0.2.1

**IPv6**:

>>> IPv6 was created to solve the shortage of addresses

>>> IPv6 addresses are 128 bit length

>>> IPv6 uses hexadecimal notation and separated by colon

>>> IPv6 supports alpha-numeric values where as IPv4 supports only numeric values

>>> IPv6 can support a vast number of addresses—about 340 undecillion

>>> Ipv6 has more security when compared to IPv4

Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

**IP address class**:

IP classes are of 5 types: A,B,C,D,E

**Class A:**

Range: 1.0.0.0 to 126.0.0.0

Purpose: For very large networks, like big companies or governments.

Format: N.H.H.H (N = Network part, H = Host part)

Number of Networks: 128 (2^7 - 2, as 0 and 127 are reserved)

Number of Hosts per Network: 16 million+ (2^24 - 2)

**Class B**

Range: 128.0.0.0 to 191.255.0.0

Purpose: For medium-sized networks, like universities or large businesses.

Format: N.N.H.H (N = Network part, H = Host part)

Number of Networks: 16,384 (2^14)

Number of Hosts per Network: 65,536 (2^16 - 2)

**Class C**

Range: 192.0.0.0 to 223.255.255.0

Purpose: For small networks, like small businesses or home networks.

Format: N.N.N.H (N = Network part, H = Host part)

Number of Networks: 2 million+ (2^21)

Number of Hosts per Network: 254 (2^8 - 2)

**Class D**

Range: 224.0.0.0 to 239.255.255.255

Purpose: For multicast groups, used in streaming and real-time communication.

Format: Not used for normal host addressing.

**Class E**

Range: 240.0.0.0 to 255.255.255.255

Purpose: Reserved for experimental use, research, and future use.

Format: Not used for normal host addressing.

**Special Addresses**

**127.0.0.1**: This is the loopback address, used to test the network interface on your own machine.

**Summary**

Class A: For very large networks.

Class B: For medium-sized networks.

Class C: For small networks.

Class D: For multicast.

Class E: Reserved for future or experimental use.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Class** | **Range** | **Purpose** | **Format** | **Number of Networks** | **Hosts per Network** | **Special Notes** |
| A | 1.0.0.0 to 126.0.0.0 | Very large networks | N.H.H.H | 128 (2^7 - 2) | 16 million+ (2^24 - 2) | Reserved: 0.x.x.x, 127.x.x.x |
| B | 128.0.0.0 to 191.255.0.0 | Medium-sized networks | N.N.H.H | 16,384 (2^14) | 65,536 (2^16 - 2) | Reserved: 128.0.x.x, 191.255.x.x |
| C | 192.0.0.0 to 223.255.255.0 | Small networks | N.N.N.H | 2 million+ (2^21) | 254 (2^8 - 2) | - |
| D | 224.0.0.0 to 239.255.255.255 | Multicast groups | - | - | - | Used for streaming, real-time |
| E | 240.0.0.0 to 255.255.255.255 | Experimental, future use | - | - | - | Reserved for research |
| **Loopback** | **127.0.0.1** | Testing network interface | - | - | - | Used to test local machine |

The IP address 127.0.0.1 is known as the loopback address

The entire block of addresses from 127.0.0.0 to 127.255.255.255 is reserved for loopback purposes.

**Public IP**: This is like a street address that everyone on the internet can see. It allows your AWS resources (like a server) to be accessible from anywhere on the internet.

**Private IP**: This is like an address within a gated community. It is used within a private network and not accessible directly from the internet.

**Elastic IP**: AWS offers a feature called Elastic IP. This is a static (unchanging) public IP address that you can attach to your AWS resources. It allows you to maintain a consistent address even if the underlying resource (like an EC2 instance) is stopped or replaced.

**Dynamic IP**: By default, AWS assigns dynamic IP addresses to resources, which can change when the resource is restarted.

Elastic IP --- Static IP --- standard IP --- It can’t be changed

Dynamic IP --- It can be change

**VPC CIDR**:

**CIDR** stands for **Classless Inter-Domain Routing**

It's a method used to specify ranges of IP addresses.

In AWS VPC, CIDR is used to define the IP address range for your virtual network.

**Example**:

VPC IP range start from 10.0.0.0, then CIDR for this VPC is 10.0.0.0/16.

we can calculate with (2^32 -n), here n= CIDR value

>>> 10.0.0.0/16 >>> CIDR value is 16, so (32-16 = 16) = 65536, total we got 65536 IP's

>>> 10.0.0.0/24 >>> CIDR value is 24, so (32-24 = 8) = 2^8 = 256, total we got 256 Ip's

**Why we use CIDR in VPC?**

We use CIDR mainly because of two reasons

>>> Defining IP address Range

>>> Efficient Addressing

**Subnet:**

subnet = subnetwork

A subnet is a smaller division of network from larger network(VPC). So that we easily manage and access network.

>>> You can divide your VPC into multiple subnets. Each subnet is a range of IP addresses within the VPC.

**Example**:

Assume VPC as a colony, in colony we have streets.

Each street is a subnet.

**Example**:

VPC: Your private colony (10.0.0.0/16 IP range).

Subnet 1 (Public Subnet): A street in colony where houses (EC2 instances) have driveways connected to the main road (internet) (10.0.1.0/24 IP range).

Subnet 2 (Private Subnet): Another street where houses are behind gates (no direct internet access) (10.0.2.0/24 IP range).

Why Use **Subnets**?

Organization: Keeps your network neat and structured.

Security: Allows for better control over who can access different parts of your network.

Redundancy: Distributes resources across multiple locations to increase reliability.

**What is Subnet CIDR?**

Subnet CIDR (Classless Inter-Domain Routing) is a way to divide a larger network into smaller, more manageable chunks. It's like splitting a big pizza into smaller slices so everyone gets their fair share.

Subnet CIDR = 192.168.1.0/24, it means we have 256 IP's

**Example**:

you have a big office network, and you want to divide it into smaller sections for different departments. You can use Subnet CIDR to do that. For example:

Marketing department: 192.168.1.0/26 (which gives you 64 IP addresses).

Sales department: 192.168.1.64/26 (another 64 IP addresses).

IT department: 192.168.1.128/26 (and so on).

In VPC CIDR we have first two octant values will be fixed rest we can change, where as in subnet CIDR first three octant will be fixed and the last will change

**Difference between VPC CIDR and Subnet CIDR**

|  |  |  |
| --- | --- | --- |
| **Aspect** | **VPC CIDR** | **Subnet CIDR** |
| Definition | Defines the overall range of IP addresses for the entire Virtual Private Cloud (VPC) | Defines the range of IP addresses available within a specific subnet within the VPC |
| Purpose | Specifies the total address space available for the VPC | Divides the VPC's address space into smaller, manageable segments |
| Scope | Encompasses the entire VPC network | Applies to individual subnetworks (subnets) within the VPC |
| Example | 10.0.0.0/16 | 10.0.0.0/24, 10.0.1.0/24, etc. |
| Number of IPs | Can potentially cover a large range of IP addresses, depending on the CIDR notation used | Covers a subset of the IP addresses available within the VPC CIDR range |
| Usage | Used to define the overall addressing scheme for the cloud network | Used to create smaller, isolated networks within the VPC for different purposes or departments |
| Analogous to | Overall land area of a country | Individual regions or states within the country |

**Internet gateway:**

IGW is establishing the connection between VPC and Internet

>>> Assume IGW is like a door between VPC and outside world(internet).

>>> IGW connects your VPC to the internet, allowing you to send and receive data to and from the outside world.

>>> Without an Internet Gateway, your VPC would be like a closed-off room with no windows or doors – it wouldn't be able to communicate with anything outside of itself.

>>> But with an Internet Gateway, it's like adding a door that lets you connect your VPC to the vast network of the internet, enabling you to access resources, websites, and services outside of your VPC, and allowing them to access resources inside your VPC if you configure it that way.

**NAT gateway:**

>>> NAT gate way in nothing but Network Address Translation.

>>> NAT gateway acts like a middleman, making sure that your device can access the internet while keeping them safe behind your router's public IP address. It translates the external communication to the appropriate devices within your network.

**Security Group**: Acts like your friend at the door, controlling traffic to and from your virtual network.

**Incoming Traffic**: Represents data packets trying to access resources in your VPC.

**Access Rules**: Are the rules you set for your security group, defining who can access what.

**Deciding Access**: Your security group decides whether to allow or block incoming traffic based on these rules.

**Inbound rule:**

>>> ncoming traffic towards the server or computer.

>>> Determines which external sources are allowed to access resources on the server or computer.

>>> Allow only specific IP addresses to connect to SSH (Secure Shell) on a server.

>>> Configured to allow access to specific ports or services required by applications running on the server.

>>> Incorrectly configured inbound rules can expose the server to security risks, such as unauthorized access or exploitation of vulnerabilities.

**Out bound rule:**

>>>Outgoing traffic originating from the server or computer.

>>> Controls which external destinations or services the server or computer is allowed to access.

>>> Allow the server to access only specific websites or services on the internet.

>>> Configured to restrict the server's access to certain websites, services, or IP addresses, based on security policies or compliance requirements.

>>> Misconfigured outbound rules can result in data breaches, unauthorized access to external resources, or the spread of malware if the server is compromised.

**Route table**:

Routing table as a map that helps network devices decide where to send data packets so they can reach their intended destinations efficiently.

**Subnet association:**

Subnet association is the practice of linking specific network resources or permissions to particular subnetworks (subnets) within a larger network. It's like assigning certain privileges or access rights to groups of devices based on their location or grouping within the network.

**Main purpose of subnet association:**

The main purpose of subnet association is to organize and manage network resources more efficiently and securely. By associating specific resources or permissions with particular subnets, network administrators can control access to those resources, enhance security by segmenting the network, and optimize network performance by directing traffic more effectively. This helps in improving overall network management, security, and performance.

**VPC peering:**

VPC peering is like connecting two private networks in the cloud so they can talk to each other directly, just as if they were on the same network.Establishing a connection between two private networks to access the data between them.

**End-point:**

An endpoint in a VPC is like a direct, private doorway that connects your virtual network to specific AWS services, allowing your resources within the VPC to securely communicate with those services without needing to go through the public internet. To establish a connection between two different services.

So, in simple terms, an endpoint in a VPC ensures secure and private communication between your VPC resources and AWS services, just like a private tunnel between two locations, keeping your data safe from the public eye.

**Network Access Control List:**

A Network Access Control List (ACL) is a set of rules used to control network traffic and enhance security within a network.

**Difference between security group and NACL?**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Security Group** | **NACL** |
| **Layer** | Instance level | Subnet level |
| **Scope** | Applied to individual resources | Applied to entire subnets |
| **Rules** | Allow rules only | Allow and deny rules |
| **Default Inbound Traffic** | Denied | Allowed |
| **Default Outbound Traffic** | Allowed | Allowed |
| **Complexity** | Easier to manage | More complex to manage |
| **Use Case** | Instance-specific access control | Subnet-specific access control |
| **Number of Rules** | More rules per security group (e.g., 60 each) | Fewer rules per NACL (e.g., 20 each) |

**Q1) How can you control the security to your VPC?**

Answer: You can use security groups and NACL (Network Access Control List) to control the security to your VPC.

**Q2) Which type of load balancer makes routing decisions at either the transport layer or the**

**Application layer and supports either EC2 or VPC.**

Answer: Classic Load Balancer

**Q3) Which is virtual network interface that you can attach to an instance in a VPC?**

Answer: Elastic Network Interface

**Q4) A Enterprise customer is starting on their migration to the cloud, their main reason for the migrating is agility and they want to the make their internal Microsoft active directory available to the many applications running on AWS, this is so internal users for only have to remember one set of the credentials and as a central point of user take control for the leavers and joiners. How could they make their actions the directory secures and the highly available with minimal on-premises on infrastructure changes in the most cost and the time-efficient way?**

Answer: By Using a VPC, they could be create an the extension to their data center and to  make use of resilient hardware IPSEC on tunnels, they could then have two domain consider to controller instances that are joined to the existing domain and reside within the different subnets in the different availability zones.

**Q5) What is VPC Peering?**

Answer: Amazon VPC peering connection is a networking connection between two amazon vpc’s that enables instances in either Amazon VPC to communicate with each other as if they are within the same network. You can create amazon VPC peering connection between your own Amazon VPC’s or Amazon VPC in another AWS account within a single region.

**Q6) When attached to an Amazon VPC which two components provide connectivity with external networks?**

Answer:

* Internet Gateway {IGW)
* Virtual Private Gateway (VGW)

**Q7) Which of the following are characteristics of Amazon VPC subnets?**

Answer:

* Each subnet maps to a single Availability Zone.
* By defaulting, all subnets can route between each other, whether they are private or public.

**Q8) Is it feasible for an EC2 exemplary occurrence to wind up an individual from a virtual private cloud?**

Answer: Amazon Virtual Private Cloud (Amazon VPC) empowers you to characterize a virtual system in your very own consistently disengaged zone inside the AWS cloud, known as a virtual private cloud (VPC). You can dispatch your Amazon EC2 assets, for example, occasions, into the subnets of your VPC. Your VPC nearly looks like a conventional system that you may work in your very own server farm, with the advantages of utilizing adaptable foundation from AWS. You can design your VPC; you can choose its IP address extend, make subnets, and arrange course tables, organize portals, and security settings. You can interface occurrences in your VPC to the web or to your own server farm

**Q9) Mention crafted by an Amazon VPC switch.**

* Answer: VPCs and Subnets. A virtual private cloud (VPC) is a virtual system committed to your AWS account. It is consistently segregated from other virtual systems in the AWS Cloud. You can dispatch your AWS assets, for example, Amazon EC2 cases, into your VPC.

**Q10) How would one be able to associate a VPC to corporate server farm?**

* Answer: AWS Direct Connect empowers you to safely associate your AWS condition to your on-premises server farm or office area over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic association. AWS Direct Connect offers committed fast, low dormancy association, which sidesteps web access suppliers in your system way. An AWS Direct Connect area gives access to Amazon Web Services in the locale it is related with, and also access to different US areas. AWS Direct Connect enables you to consistently parcel the fiber-optic associations into numerous intelligent associations called Virtual Local Area Networks (VLAN). You can exploit these intelligent associations with enhance security, separate traffic, and accomplish consistence necessities.

**Q11) What are the Defaults services we get when we create custom AWS VPC?**

Answer:

* Route Table
* Network ACL
* Security Group

**Q12) How do you access the Ec2 which has private IP which is in private Subnet?**

Answer: We can access using VPN if the VPN is configured into that Particular VPC where Ec2 is assigned to that VPC in the Subnet. We can access using other Ec2 which has the public access.

**Q13) We have a custom VPC Configured and MYSQL Database server which is in Private Subnet and we need to update the MYSQL Database Server, What are the Option to do so.**

Answer: By using NAT Gateway in the VPC or Launch a NAT Instance (Ec2) Configure or Attach the NAT Gateway in Public Subnet (Which has Route Table attached to IGW) and attach it to the Route Table which is Already attached to the Private Subnet.

**Q14) To establish a peering connection between two VPC’s What condition must be met?**

Answer:

* CIDR Block should not overlap
* VPC should be in the same region
* VPC must belong to same account.
* CIDR block should not overlap between vpc setting up a peering connection. peering connection is allowed within a region, across region, across different account.

**Q15) Maximum number of EC2 which can be created in VPC.**

* Answer: **Maximum 20 instances can be created in a VPC**. we can create 20 reserve instances and request for spot instance as per demand.

Tell me the scope of the VPC market?

Ans: Scopes are: Agility Security. Easy hybrid cloud deployment. More performance. Customer Satisfaction. More resources in channel innovation.

9. Tell me the basic difference between VPC and VPN?

Ans: VPC is from Amazon Web Services. It has been created as per zone for giving access to clients. It depends on multiple Subnet. But a VPN is a gateway, actually. This is the access point of the VPN network.

10. How many VPC can be created in AWS Zone?

Ans: You can create by default only 5 VPC in a single AWS zone.

13. Tell me about the advantages of AWS VPC?

Ans: There are a few advantages, they are: Provide a complete process to build a virtual network. No need for hardware, any physical data center, or VPN. Full power access with control over your network. EC2 instance is available to connect to the internet. Can do enhanced security level in VPC with EC 2 instances.

17. Is it secure if we run an EC2 instance with AWS VPC?

Ans: AWS EC2 instances are very secure for the AWS VPC network. It can control both inbound and outbound traffic in the same zone. Once the EC2 instance declined any traffic, further, that traffic is not allowed.

19. How can you find out the available zones for your Subnet?

Ans: Always keep remembering that while we are creating a subnet we need to mention the available zone. By using VPC Wizard, we can choose an available zone for the subnet. We can specify the available zone by using the API or CLI. If we don’t mention the available zone, then by default no permission options will be activated. The system will be choosing the available zone.

22. Do we need prior knowledge to use them by default VPC?

Ans: The answer is no. We can find out about it from the AWS management console in a by-fault VPC. AWS used to create one by default VPC. We need to create a default subnet for each available zone. Default VPC will be connected to the internet through the gateway automatically.

26. Do you think that we can delete the default VPC?

Ans: Yes, we can delete it from the AWS console, in that case, if we connect with the AWS support team then they can help us to retrieve the old default VPC.

**Basic Questions**

**What is a VPC in AWS?**

A Virtual Private Cloud (VPC) allows you to provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.

What are the components of a VPC?

Components include subnets, route tables, internet gateways, NAT gateways, security groups, network ACLs, and VPC endpoints.

**What is a subnet and how is it used in VPC?**

A subnet is a range of IP addresses in your VPC. Subnets can be public (accessible from the internet) or private (not accessible from the internet).

**What is the difference between a security group and a network ACL?**

Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. Network ACLs (Access Control Lists) act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

**Explain the purpose of an Internet Gateway (IGW).**

An IGW allows communication between instances in your VPC and the internet.

**What is a route table and how does it function in VPC?**

A route table contains a set of rules, called routes, that are used to determine where network traffic is directed. Each subnet in your VPC must be associated with a route table.

**Intermediate Questions**

**What is a NAT Gateway and why is it used?**

A NAT Gateway enables instances in a private subnet to connect to the internet or other AWS services but prevents the internet from initiating a connection with those instances.

**Can you have more than one internet gateway in a VPC?**

No, you can only attach one internet gateway to a VPC at a time.

**What are VPC endpoints?**

VPC endpoints allow you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

**Explain the difference between a VPC Peering Connection and a VPN Connection.**

A VPC Peering Connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. A VPN Connection is used to establish a secure, encrypted connection over the internet between your on-premises network and your VPC.

**What is an Elastic IP and how is it used in a VPC?**

An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. It is associated with your AWS account and can be used to mask the failure of an instance or software by rapidly remapping the address to another instance.

**Describe the use of flow logs in VPC.**

Flow logs capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3.

**Advanced Questions**

**How would you set up a VPC for a multi-tier application?**

For a multi-tier application, you might create several subnets within a VPC: one for the web tier (public subnet), one for the application tier (private subnet), and one for the database tier (private subnet). Security groups and network ACLs would be configured to control traffic between these subnets.

**How do you connect multiple VPCs across different regions?**

You can connect multiple VPCs across different regions using VPC Peering or AWS Transit Gateway with inter-region peering.

**What is AWS Transit Gateway and how does it differ from VPC Peering?**

AWS Transit Gateway enables you to connect your VPCs and on-premises networks through a central hub. It simplifies network architecture and reduces the complexity of managing multiple VPC peering connections.

**How can you achieve high availability and redundancy in a VPC?**

Achieve high availability and redundancy by deploying resources across multiple Availability Zones (AZs), using Elastic Load Balancers, Auto Scaling groups, and multi-AZ deployments for databases.

**Explain the concept of VPC sharing and when you would use it.**

VPC sharing allows multiple AWS accounts to create their application resources, such as Amazon EC2 instances, Amazon RDS databases, and Amazon Redshift clusters, into shared, centrally managed VPCs. It is useful for managing resources in large, multi-account AWS environments.

**What security measures would you implement in a VPC?**

Security measures include configuring security groups, network ACLs, enabling VPC Flow Logs, using AWS Identity and Access Management (IAM) roles and policies, and employing encryption for data at rest and in transit.

**Practical Scenario Questions**

**How would you troubleshoot connectivity issues in a VPC?**

Troubleshooting steps include checking security group rules, network ACL rules, route tables, VPC peering connections, NAT gateways, and verifying that the necessary ports are open.

**How can you ensure data security between instances in different VPCs?**

Ensure data security by using VPC peering with restrictive security group rules, VPN connections, or AWS Direct Connect with encryption protocols.