# What is VPC:

* AWS VPC (Virtual Private Cloud) is a cloud computing service offered by Amazon Web Services (AWS) that allows users to create a virtual private network within the AWS cloud infrastructure.
* Essentially, it allows users to launch resources like EC2 instances, RDS databases, and more, within their own isolated network.
* When we create a VPC, it is recommended to specify a CIDR block from the private IPv4 address ranges as specified in RFC 1918

|  |  |
| --- | --- |
| **RFC 1918 Range** | **Example CIDR Block** |
| 10.0.0.0 - 10.255.255.255(10/8 prefix) | 10.0.0.0/16 |
| 172.16.0.0 - 172.31.255.255(172.16/12  Prefix) | 172.31.0.0/16 |
| 192.168.0.0 -  192.168.255.255(192.168/16  prefix) | 192.168.0.0 |

# Features of VPC:

The following features help you configure a VPC to provide the connectivity that your application need:

**Virtual Private Cloud(VPC):** A VPC is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud.

* After you create a VPC, you can add subnets

**Subnets:** A Subnet is a range of IP addresses in your VPC.

* A Subnet must reside in a single availability zone.
* After you add subnets, you can deploy AWS resources in your VPC.

# IP Addressing:

* You can assign IPv4 addresses and IPv6 addresses to your VPCs and Subnets
* You can also bring your public IPv4 and IPv6 GUA addresses to AWS and allocate them to resources in your VPC, such as Ec2 instances, NAT Gateways, and Network Load Balancers.

# Routing:

* Use Route tables to determine where network traffic from your subnet or gateway is directed.

# Gateway and Endpoints:

* A gateway connects your VPC to another network
* For example, use an internet gateway to connect your VPC to the internet.
* Use a VPC endpoint to connect to AWS services privately, without the use of an internet gateway or NAT device

# Peering Connections:

* Use a VPC peering condition to route traffic between the resources in two VPCs

# VPC Flow Logs:

* A flow log captures information about the IP traffic going to and from network interfaces in your VPC

# VPN Connections:

* Connect your VPCs to your On-premises networks using AWS Virtual Private Network (AWS VPN)

# What is CIDR:

* CIDR stands for Classless Inter-Domain Routing
* The CIDR block represents the IP address range that will be used for the VPC, and determines the number of IP addresses that are available for use within the VPC.
* When choosing the CIDR block for an AWS VPC, users must specify the IP address range for the VPC
* For example, a CIDR block of 10.0.0.0/16 represents an IP address range of 10.0.0.0 to 10.0.255.255, and provides a total of 65,536 IP addresses for use within the VPC.
* In addition to IPv4 addresses, AWS also supports IPv6 addresses, IPv6 is the next generation of IP addresses, and provides a much larger address space than IPv4. In AWS, users can choose to use either IPv4 or IPv6 addresses for their VPC, depending on their requirements.

# What is Subnets:

* IN AWS VPC, a subnet is a range of IP addresses within the VPC’s IP address range that can be used to launch resources like EC2 instances, RDS databases, and more.
* Subnets allow users to segment their VPC into smaller, more manageable networks, and provide a way to control network traffic within the VPC

# Types of Subnets:

Depending on how you configure your VPC, subnets are considered public, private, or VPN-Only

# Public Subnet:

* The subnet traffic is routed to the public internet through an internet gateway or an egress-only internet gateway

# Private Subnet:

* The subnet traffic can’t reach the public internet through an internet gateway or egress-only internet gateway.
* Access to the public internet requires a NAT device

# VPN Only Subnet:

* The Subnet traffic is routed to Site-to-Site VPN Connection through a Virtual private gateway. The subnet traffic can’t reach the public internet through an internet gateway.

# Subnet Sizing for IPv4:

* The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR Block for the VPC (to create multiple subnets in the VPC)
* The allowed block size is between a /28 netmask and /16 netmask.
* If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.
* For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses.
* You can break this CIDR block into two subnets, each supporting 128 IP addresses
* One subnet users CIDR block 10.0.0.0/25 (for addresses

10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255)

* The first four IP addresses and the last IP address in each subnet CIDR block are not available for your use, and they cannot be assigned to a resource, such as an EC2 instance
* For Example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:
  + 10.0.0.0: Network Address
  + 10.0.0.1: Reserved by AWS for the VPC Router
  + 10.0.0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two.
  + 10.0.0.3: Reserved by AWS for future use
  + 10.0.0.255: Network broadcast address. We don't support broadcast in a VPC, therefore we reserve this address.

# Subnet Routing:

* Each subnet must be associated with a route table, which specifies the allowed routes for outbound traffic leaving the subnet
* Every subnet that you create is automatically associated with the main route table for the VPC
* You can change the association, and you can change the contents of the main route table

# What is Route Table:

* In AWS VPC, a route table is a set of rules that determine how traffic is routed between subnets within the VPC and to the internet
* Each subnet within a VPC is associated with a route table, which contains a set of rules that define the traffic flow for the subnet.

# Route Table Components:

The Components of an AWS VPC route table include:

# Route Entries:

* These are the rules that define how traffic is routed based on the destination IP address
* Each route entry consists of a destination CIDR block (the IP address range for the destination) and a target (the destination for the traffic)

# Subnet Associations:

* Each subnet within a VPC is associated with a specific route table. This determines which set of route entries will be used to route traffic for resources within that subnet.

# Main Route Table:

* Each VPC has a default route table (known as the main route table) that is used for all subnets that are not explicitly associated with a custom route table

# Custom Route Tables:

* Users can create custom route tables to control the flow of traffic for specific subnets within the VPC.

# What is Internet Gateway (IGW):

* In AWS, an Internet Gateway (IGW) is a horizontally scaled, redundant, and highly available VPC (Virtual Private Cloud) component that allows resources within a subnet to communicate with the Public internet.
* An internet gateway serves as a gateway for traffic that is destined for the internet, and is typically the target for a route entry that directs traffic from a Public subnet to the internet
* It supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic.
* There’s no additional charge for creating an internet gateway.