Components of Amazon VPC

Amazon VPC comprises a variety of objects that will be familiar to customers with existing networks:

- A Virtual Private Cloud: A logically isolated virtual network in the AWS cloud. You define a VPC's IP address space from the ranges you select.
- Subnet: A segment of a VPC's IP address range where you can place groups of isolated resources.
- Internet Gateway: The Amazon VPC side of a connection to the public Internet.
- NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.
- Route Table: A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed.
- DNS Hostname: The Amazon DNS server resolves a public DNS hostname to the public IPv4 address of the instance outside the network of the instance.
- CIDR: Classless Inter-Domain Routing

IP Address:

- **Class A:** IP addresses are those between 0.0.0.0 and 127.255.255.255.
- **Class B:** IP addresses are those between 128.0.0.0 and 191.255.255.255.
- **Class C:** IP addresses are those between 192.0.0.0 and 223.255.255.255.

Each IP address class has a matching **"subnet mask," which is an easy way of identifying which part of the IP address relates to the network and which part relates**

to the host. This is essential to ensure packets traveling through the network get to the right place.

The default matching subnet masks for each subnet class are as follows:

- **Class A:** 0.0.0
- **Class B:** 255.0.0
- **Class C:** 255.255.0

IP Address Class	# Subnet Bits	Subnet Mask	# Addresses	Example IP Address Range
Class A	8	255.0.0.0	16,777,216	10.0.0.0 - 10.255.255.255
Class B	16	255.255.0.0	65,534	192.168.1.0 - 192.168.1.255
Class C	24	255.255.255.0	254	10.5.1.0 - 10.5.1.255

VPC Highlights

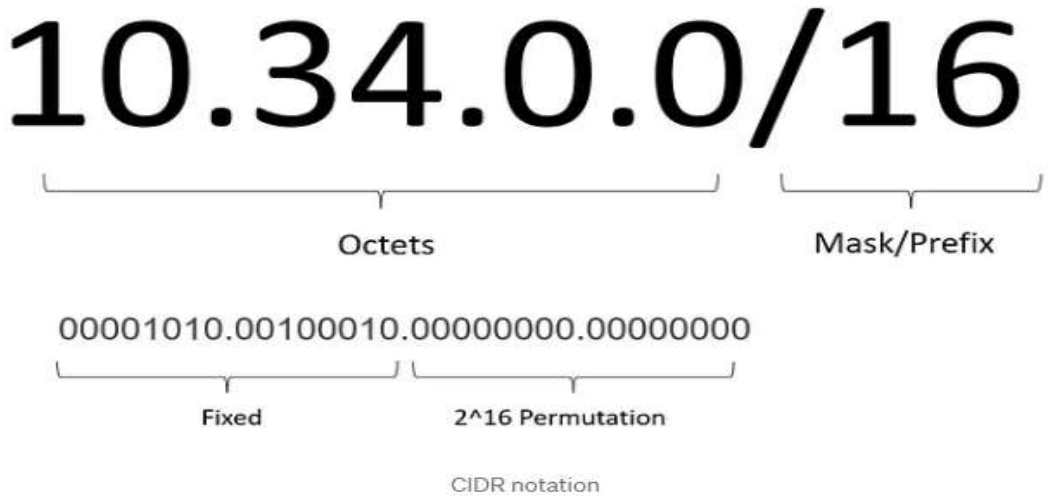
- A VPC is a logically isolated piece of AWS cloud dedicated to your company. This means, you can run applications on overly provisioned, highly available, and redundant infrastructure setup and it is managed by AWS. All the complexity of setting up a data center with cables, server racks, hardware, power supply, etc. all are managed by AWS.
- A VPC belongs to a region.
- A VPC spans all availability zones.
- You can have multiple VPCs per region.
- VPC contains one or more subnets.
- A Subnet is tied to a single availability zone.
- EC2 instances launch into subnets.

CIDR:

Classless Inter-Domain Routing (CIDR) is an IP address allocation method that improves data routing efficiency on the internet. Every machine, server, and end-user device that connects to the internet has a unique number, called an IP address, associated with it

Organizations use CIDR to allocate IP addresses flexibly and efficiently in their networks.

To create a VPC we need to supply a Classless Inter-Domain Routing (CIDR) block. Our VPC must be /16 or smaller. We need to be careful in selecting the right size of VPC as we can not modify the range of an existing CIDR block.



CIDR notation

An IPv4 address is represented as four 8-bit decimal numbers or octets separated by dots. Prefix number (Mask) is the number of bits locked from the left side. In the above example, the first 16 bits are fixed. The remaining (32 -16=16) bits' permutations will decide the IPs in the subnet.

Route table

Every resource created in a subnet gets a private IP address from the CIDR of the subnet. And instances communicate with each other using this IP. How to reach a particular IP is defined in the subnets associated route table.

The table has the following structure. A destination and the target for the destination.

Destination	Target
10.31.98.1/24	pcx-08xxxxxxx
10.30.2.0/20	local
10.49.192.0/20	vgw-7xxxxxx
0.0.0.0/0	nat-0xxxxxxx
pl-63xxxx	vpce-7xxxxx
0.0.0.0/0	igw-bxxxxxx

Route table

If our route table has multiple routes, the most specific route that matches the traffic (longest prefix match) will be applied. Let us say we want to reach 10.1.1.24 and in the route table, we have two routes, one for 10.1.1.0/24 and the other 10.1.0.0/16, then it will use the first one.

NAT Gateway

We saw that resources in the private subnet cant be reached from the internet and they also cant reach the internet. But we need access to the internet for various use cases like downloading software. To enable the host from the private subnet to reach the internet we use NAT.

NAT device enables instances in a private subnet to connect to the internet but prevents hosts on the internet from initiating connections with the instances. NAT does the Address translation from private IP to its own public IP. Must be created in a public subnet for accessing internet addresses.