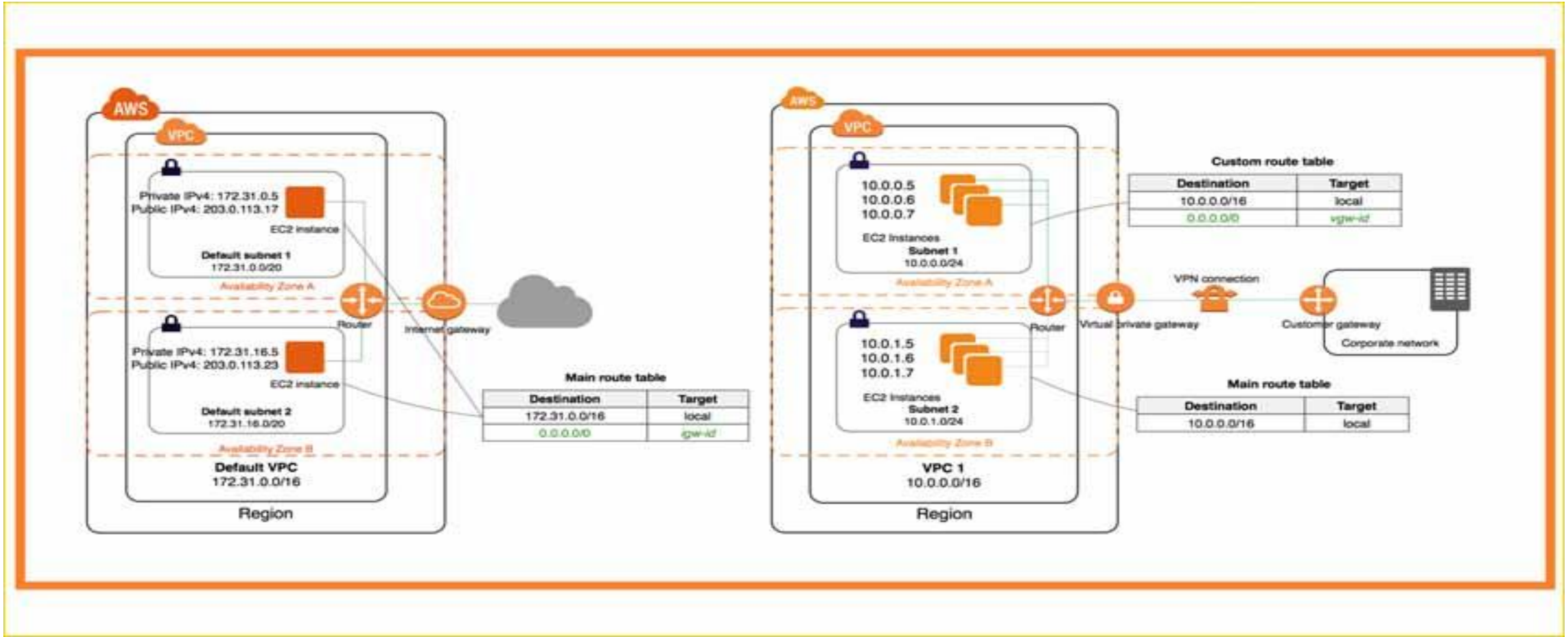
CLICK HERE
TO
WATCH THE TUTORIAL

1) What is AWS VPC?
2) What is Subnetting ?
3) What are The Important Components of Subnetting?
4) What is AWS VPC Subnetting?
5) Why do we need AWS VPC Subnetting?
6) Simplifying AWS VPC Subnetting

AWS VPC Subnetting Simplified

What is AWS VPC?

Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.



Main route table

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-id

Custom route table

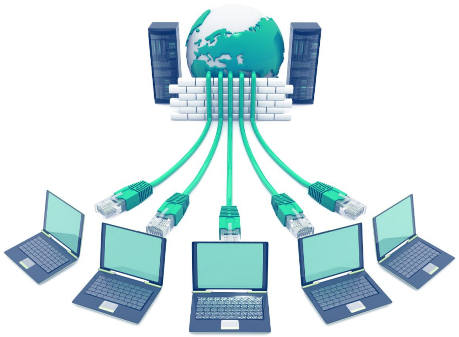
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	vgw-id

Main route table

Destination	Target
10.0.0.0/16	local

What is Subnetting

To understand what Subnetting is, first we have to understand what exactly is the Network and Subnet

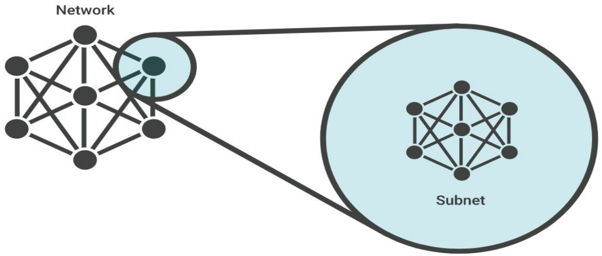


What is Network?

A network is a group of two or more connected computing devices. Usually all devices in the network are connected to a central hub — for instance, a router. A network can also include subnetworks, or smaller subdivisions of the network

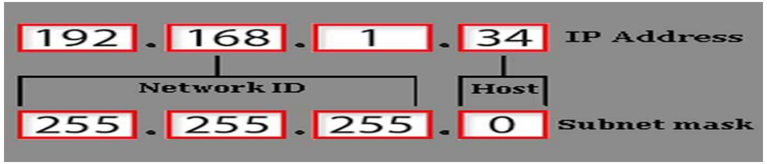
What is Subnet ?

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.



What is Subnetting ?

Subnetting/Subnetworking is how very large networks, such as those provided by ISPs, are able to manage thousands of IP addresses and connected devices.
In simple words: Dividing bigger networks into smaller networks called Subnetting.



192 . 168 . 1 . 34 IP Address

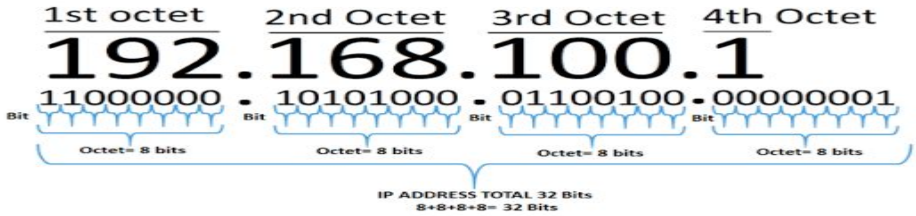
Network ID | Host

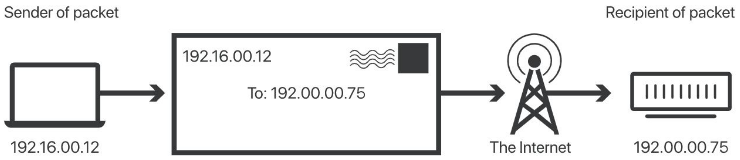
255 . 255 . 255 . 0 Subnet mask

Important Components of Subnetting

IP Address:

Every device that connects to the Internet is assigned a unique IP (Internet Protocol) address, enabling data sent over the Internet to reach the right device out of the billions of devices connected to the Internet. While computers read IP addresses as binary code (a series of 1s and 0s), IP addresses are usually written as a series of alphanumeric characters.
E.g. 115.96.140.123 or 192.168.100.1





Subnet Mask

A subnet mask is like an IP address, but for only internal usage within a network. Routers use subnet masks to route data packets to the right place. Subnet masks are not indicated within data packets traversing the Internet — those packets only indicate the destination IP address, which a router will match with a subnet.

In this analogy, "Ramesh" is like an IP address and "Cloud Support" is like a subnet mask. By matching Ramesh to his department, Suresh's letter was quickly sorted into the right group of potential recipients. Without this step, office administrators would have to spend time laboriously looking for the exact location of Ramesh's desk, which could be anywhere in the building.

E.g. IP packet is addressed to the IP address 192.0.2.15. This IP address is a Class C network, so the network is identified by "192.0.2" (or to be technically precise, 192.0.2.0/24). Network routers forward the packet to a host on the network indicated by "192.0.2."Once the packet arrives at that network, a router within the network consults its routing table. It does some binary mathematics using its subnet mask of 255.255.255.0, sees the device address "15" (the rest of the IP address indicates the network), and calculates which subnet the packet should go to. It forwards the packet to the router or switch responsible for delivering packets within that subnet, and the packet arrives at IP address 192.0.2.15

Important Components of Subnetting

Classless Inter-Domain Routing (**CIDR**)

Classless Inter-Domain Routing (**CIDR**) is a method for allocating IP addresses and for IP routing. **The Internet Engineering Task Force** introduced CIDR in 1993 to replace the previous classful network addressing architecture on the Internet. Its goal was to slow the growth of routing tables on routers across the Internet, and to help slow the rapid exhaustion of IPv4 addresses. -- **Wikipedia**

The original classful network design of the internet included inefficiencies that drained the pool of unassigned IPv4 addresses faster than necessary. The classful design included the following:

- Class A, with over 16 million identifiers
- Class B, with 65,535 identifiers
- Class C, with 254 host identifiers

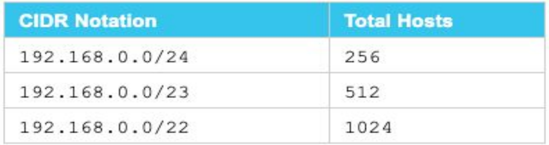
If an organization needed more than 260 host machines, it would be switched into Class B. However, this could potentially waste over 60,000 hosts if the business didn't need to use them, thus unnecessarily decreasing the availability of IPv4 addresses. CIDR was introduced to fix this problem.

CIDR notation

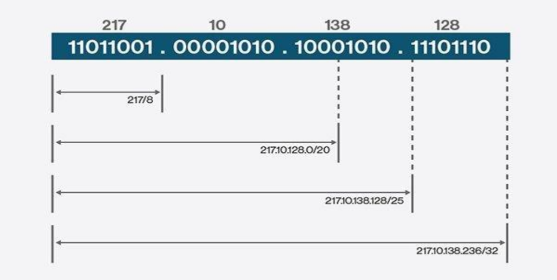
CIDR notation is a compact representation of an IP address and its associated network mask.CIDR notation specifies an IP address, a slash ('/') character, and a decimal number. The decimal number is the count of leading *1* bits in the network mask. The number can also be thought of as the width (in bits) of the network prefix. The IP address in CIDR notation is always represented according to the standards for IPv4 or IPv6.

The idea is that you can add a specification in the IP address itself as to the number of significant bits that make up the routing or networking portion.

For example, we could express the idea that the IP address 192.168.0.15 is associated with the netmask 255.255.255.0 by using the CIDR notation of 192.168.0.15/24. This means that the first 24 bits of the IP address given are considered significant for the network routing.



CIDR Notation	Total Hosts
192.168.0.0/24	256
192.168.0.0/23	512
192.168.0.0/22	1024



Source: Technology Training Ltd.

CIDR is based on variable-length subnet masking (VLSM), which enables network engineers to divide an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnetworks with different host counts without wasting large numbers of addresses.

CIDR addresses are made up of two sets of numbers: a prefix, which is the binary representation of the network address -- similar to what would be seen in a normal IP address -- and a suffix, which declares the total number of bits in the entire address. For example, CIDR notation may look like: 192.168.129.23/17 -- with 17 being the number of bits in the address. IPv4 addresses allow a maximum of 32 bits.

Important Components of Subnetting

CIDR Block

The prefix, first group of bits in the notation allows you to group the multiple blocks of network addresses into a single routing network. CIDR blocks share the first group of bits (the binary representation of the network addresses). The blocks are also identified using same decimal dot notation system as IPv4 addresses.
For example, a CIDR block is shown below
10.0.1.0/24
Here /24 signifies the total number of 1's bits in the routing mask (network mask).
This IP address can be shown as below in the binary format:
11111111.11111111.11111111.00000000
Here the first 24 bits are marked as 1.
It would be equivalent to a network mask of 255.255.255.0
Note that the network addresses that have the identical prefix and the same number of bits, always belong the same block. Also, the large and small blocks can be distinguished by the length of the prefix.

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

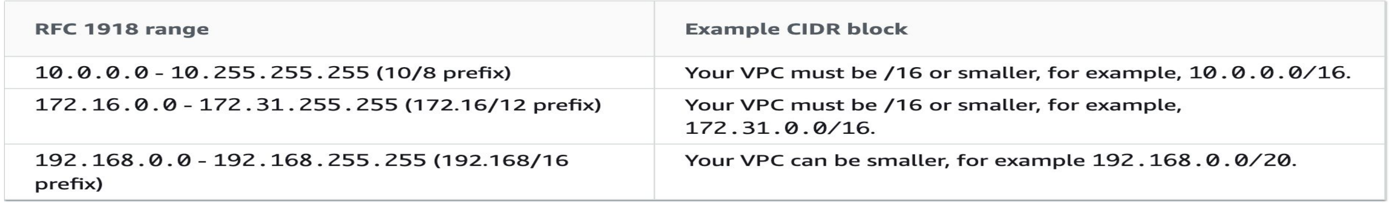
What is AWS VPC Subnetting ?

AWS VPC Subnetting:

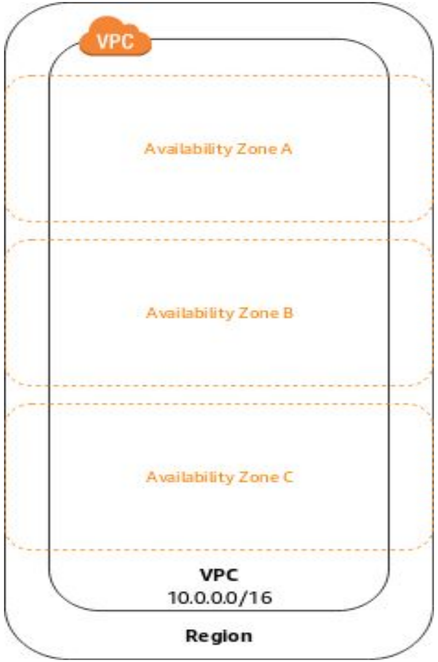
A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. A VPC spans all of the Availability Zones in the Region. After creating a VPC, you can add one or more subnets in each Availability Zone, this is called AWS VPC Subnetting.

When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block as per RFC 4632.; for example, 10.0.0.0/16. This is the primary CIDR block for your VPC.

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:



RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	Your VPC must be /16 or smaller, for example, 10.0.0.0/16.
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	Your VPC must be /16 or smaller, for example, 172.31.0.0/16.
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	Your VPC can be smaller, for example 192.168.0.0/20.



Key Points

- The allowed range of CIDR block size for the VPC (Virtual Private Cloud) is between a /16 network mask (65,536 IP addresses) and /28 network mask (16 IP addresses).
- The CIDR block of a subnet can be same as that of the block for the VPC (for a single subnet in the VPC)
- The CIDR block of a subnet can also be same as that of the other subset in case of multiple subnets.
- In a subnet CIDR block, the first four IP addresses and the last IP address in each subnet block are not available to use, and cannot be assigned to an instance. For example, in a subnet with 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.
  - 10.0.0.3: Reserved by AWS for future use.
  - 10.0.0.255: Network broadcast address.

Why AWS VPC Subnetting Needed?

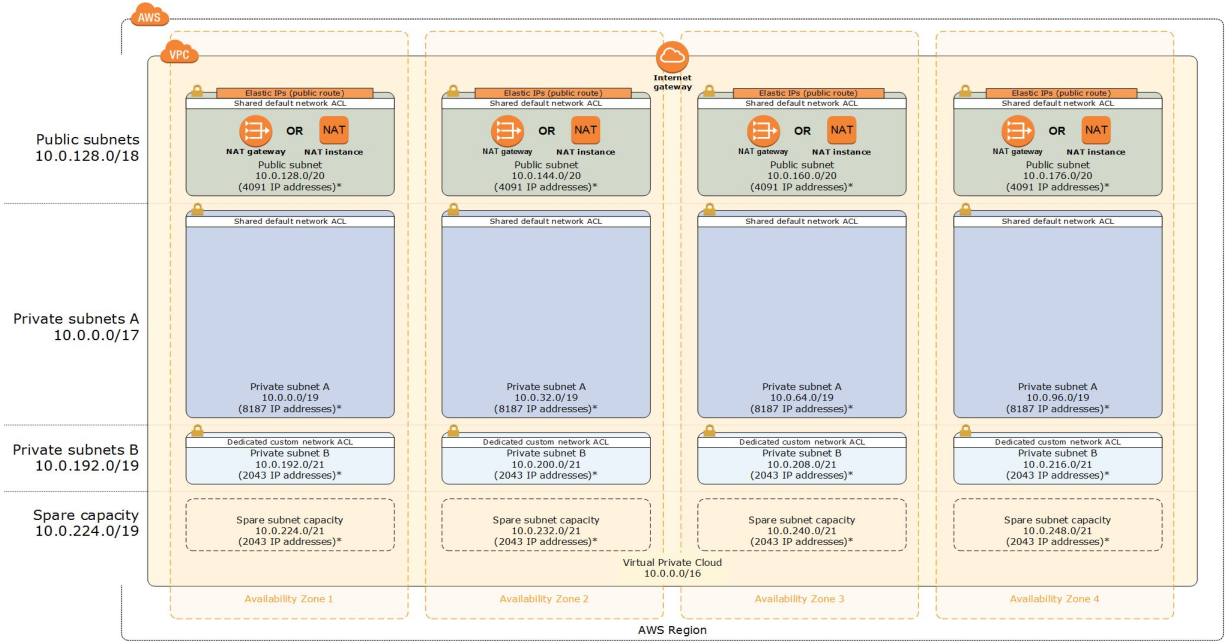
Why we exactly need AWS VPC Subnets?

When you create a subnet, you specify the **CIDR block** for the subnet, which is a subset of the VPC CIDR block.

Each subnet must reside entirely within **one Availability Zone** and **cannot span zones**.

Availability Zones are distinct locations that are **engineered to be isolated from failures** in other Availability Zones.

By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. AWS assign a unique ID to each subnet.



AWS
VPC
Internet gateway
Public subnets 10.0.128.0/18
Private subnets A 10.0.0.0/17
Private subnets B 10.0.192.0/19
Spare capacity 10.0.224.0/19
Elastic IPs (public route)
Shared default network ACL
OR
NAT
NAT gateway
NAT instance
Public subnet 10.0.128.0/20 (4091 IP addresses)*
Public subnet 10.0.144.0/20 (4091 IP addresses)*
Public subnet 10.0.160.0/20 (4091 IP addresses)*
Public subnet 10.0.176.0/20 (4091 IP addresses)*
Private subnet A 10.0.0.0/19 (8187 IP addresses)*
Private subnet A 10.0.32.0/19 (8187 IP addresses)*
Private subnet A 10.0.64.0/19 (8187 IP addresses)*
Private subnet A 10.0.96.0/19 (8187 IP addresses)*
Dedicated custom network ACL
Private subnet B 10.0.192.0/21 (2043 IP addresses)*
Private subnet B 10.0.200.0/21 (2043 IP addresses)*
Private subnet B 10.0.208.0/21 (2043 IP addresses)*
Private subnet B 10.0.216.0/21 (2043 IP addresses)*
Spare subnet capacity 10.0.224.0/21 (2043 IP addresses)*
Spare subnet capacity 10.0.232.0/21 (2043 IP addresses)*
Spare subnet capacity 10.0.240.0/21 (2043 IP addresses)*
Spare subnet capacity 10.0.248.0/21 (2043 IP addresses)*
Virtual Private Cloud 10.0.0.0/16
Availability Zone 1
Availability Zone 2
Availability Zone 3
Availability Zone 4
AWS Region

*Note that the IP addresses exclude the five (5) IP addresses from each subnet that are reserved and unavailable for use.

© 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Note:

If a subnet's **traffic is routed to an internet gateway**, the subnet is known as a ***public subnet***

If a subnet **doesn't have a route to the internet gateway**, the subnet is known as a ***private subnet***

Simplifying AWS VPC Subnetting

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 (for multiple subnets). 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 uses 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).
Note: Always remember 5 IP addresses reserved and not useable, as follows:

10.0.0.0/25	10.0.0.128/25
10.0.0.0: Network address.	10.0.0.128: Network address.
10.0.0.1: Reserved by AWS For VPC Router	10.0.0.129: Reserved by AWS For VPC Router
10.0.0.2: Reserved by AWS for DNS Server	10.0.0.130: Reserved by AWS for DNS Server
10.0.0.3: Reserved by AWS for future use	10.0.0.131: Reserved by AWS for future us
10.0.0.127: Network broadcast address. But note, AWS VPC don't support broadcast, that's why reserved	10.0.0.255: Network broadcast address. But note, AWS VPC don't support broadcast, that's why reserved

So here available ip in each subnet will be = 128 - 5 = 121 IPs each
Utilize Subnet Calculator ot CIDR Calculator to Create Subnets

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

CIDR Block Adding Rules

- The allowed block size is between a /28 netmask and /16 netmask.
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
- You cannot increase or decrease the size of an existing CIDR block.
- You have a quota on the number of CIDR blocks you can associate with a VPC and the number of routes you can add to a route table. You cannot associate a CIDR block if this results in you exceeding your quotas, more details here
- The CIDR block must not be the same or larger than a destination CIDR range in a route in any of the VPC route tables. For example, in a VPC where the primary CIDR block is 10.2.0.0/16, you have an existing route in a route table with a destination of 10.0.0.0/24 to a virtual private gateway. You want to associate a secondary CIDR block in the 10.0.0.0/16 range. Because of the existing route, you cannot associate a CIDR block of 10.0.0.0/24 or larger. However, you can associate a secondary CIDR block of 10.0.0.0/25 or smaller.

Good luck!

I hope you'll use this knowledge and build awesome solutions.

If any issue contact me in Linkedin: https://www.linkedin.com/in/sandip-das-developer/

Or mail me: **contact@sandipdas.in**

Subscribe My Youtube Channel here: http://bit.ly/LearnWithSandip