**VPC** (Virtual private cloud)

A **VPC (Virtual Private Cloud)** in AWS is a secure, isolated network in the cloud where you can run and control your resources, such as servers and databases, with customizable IP ranges, subnets, and security settings.

Classless Inter-Domain Routing

an **IPv4 CIDR** (Classless Inter-Domain Routing) block in AWS defines the range of IP addresses that your **Virtual Private Cloud (VPC)** can use

1. **Automatic IP Assignment**: When you launch something like an EC2 instance, AWS instantly assigns it an IP address from your VPC’s CIDR range, so it can start communicating right away.
2. **Control Connections**: You can divide your VPC into sections (subnets) to control which resources can talk to each other. For example, you can keep your web servers separate from your database servers. These rules apply immediately.
3. **Access and Security Rules**: You can set up rules to allow or block specific traffic, like blocking outside Internet access for private resources. These security settings work instantly. **Class**

**Class A**: 1.0.0.0 to 126.0.0.0

**Class B**: 128.0.0.0 to 191.255.0.0

**Class C**: 192.0.0.0 to 223.255.255.0

**Class D**: 224.0.0.0 to 239.255.255.255 (Multicast)

**Class E**: 240.0.0.0 to 255.255.255.255 (Experimental)

When we increase the number then we will decrease the host of the application

A **VPC** is created at the **region** level, and **subnets** are created within **specific Availability Zones** in that region.

* Every subnet will have 255 IP address

**How CIDR Notation Works:**

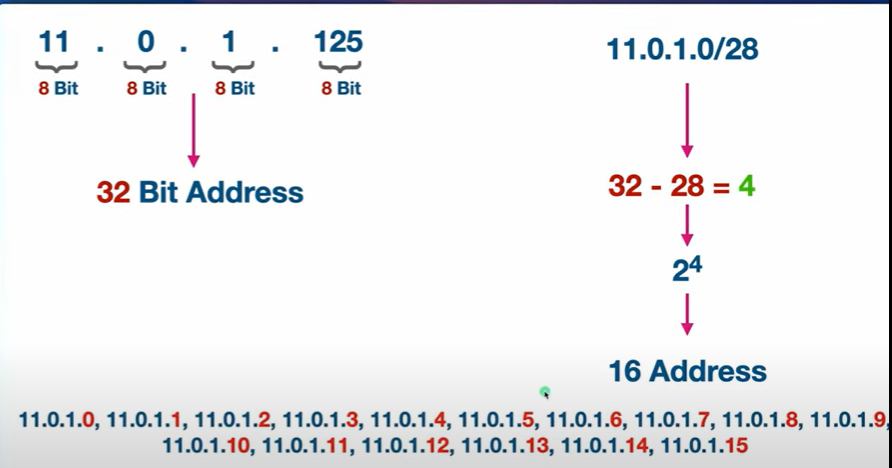
1. **IP Address and Prefix**: CIDR notation combines an IP address with a **prefix length** that indicates how many bits are used for the network part of the address. For example:
   * 192.168.1.0/24
   * Here, 192.168.1.0 is the IP address, and /24 is the prefix length, meaning the first 24 bits are for the network portion.

2. **Prefix Length**:

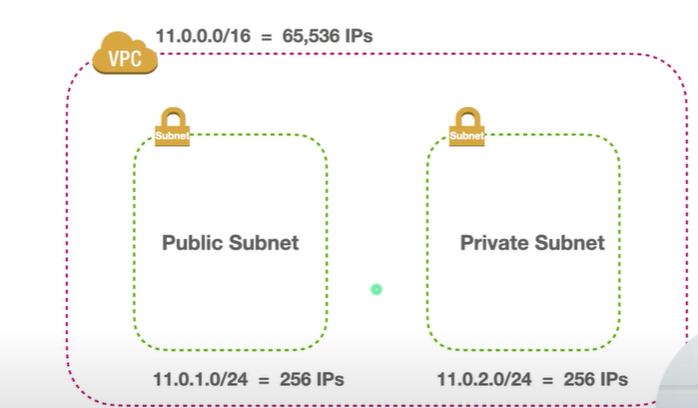
* + The **prefix length** (number after the slash) defines how many bits are fixed as the network portion.
  + The remaining bits are used for host addresses within that network.
  + The smaller the prefix number, the larger the network; the larger the prefix number, the smaller the network.
* /24 provides 256 IP addresses
* /16 provides 65,536 IP addresses.
* /32 specifies a single IP address.
* When we increase the number then we will decrease the host of the application

**How are we calculating the addresses?**

11.0.0.0/24 = 256 IP ADDRESSES



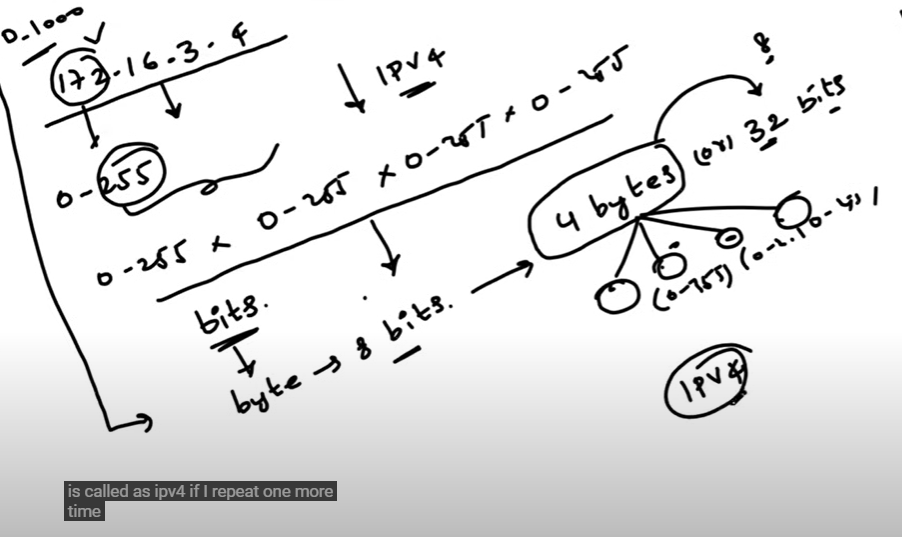
VPC is a big component



Ip address

It is used to generate a unique address for a device that is connected to your network

The ipv4/ipv6 is used to create unique numbers for all devices



0-255

Subnet

A **subnet** (short for *subnetwork*) is a smaller network within a larger network. In simple terms, it divides a large network into smaller, more manageable sections

* Security
* Privacy
* Isolation

They two type of subnet

* Public subnet = it having access to internet
* Private subnet = it doesn't access to internet

How to convert public to private

* Vpc →routetable →internetgateway

Creating private Vpc

Creating Peering connection

Create a order in

Create ec2 instances

Create my sql

**VPC Flow Overview (Simplified)**

A Virtual Private Cloud (VPC) is a secure network within AWS that allows you to launch and manage resources, such as servers and databases. Here’s a simplified flow from a user accessing an application within a VPC:

1. **User Request**  
   A user sends a request to access an application hosted on AWS (e.g., a website or service).
2. **Internet Gateway (IGW)**
   * The request enters the VPC through the Internet Gateway if it comes from the internet.
   * The IGW allows public internet access.
3. **Route Table**
   * The route table directs traffic within the VPC.
   * It determines where the request should go next (public or private subnet).
4. **Public Subnet**
   * Contains resources accessible from the internet, like a Load Balancer or a Web Server.
   * Requests may pass through a Load Balancer to manage and distribute traffic.
5. **Private Subnet**
   * Contains secure resources, like application servers or databases, that are not directly accessible from the internet.
6. **Network Access Control List (NACL)**
   * Provides an additional layer of security at the subnet level by controlling inbound and outbound traffic.
7. **Security Group**
   * Acts as a virtual firewall for individual instances (like EC2).
   * Controls which traffic is allowed to reach specific servers or applications.
8. **Application Server (EC2 Instance)**
   * The final destination where the application is hosted.
   * The server processes the user’s request and returns the appropriate response.

**NACL (Network Access Control List) – Subnet-Level Security**

NACLs provide another layer of security, controlling traffic at the subnet level.

* Apply rules to allow or deny traffic for all instances in a subnet.
* Unlike Security Groups, NACLs are **stateless**:
  + Rules must be set for both inbound and outbound traffic.
* Example: Denying all traffic from a suspicious IP address for an entire subnet.

**Security Groups – Instance-Level Security**

Security Groups act as virtual firewalls for EC2 instances.

* Define rules to control **inbound** (incoming) and **outbound** (outgoing) traffic.
* By default:
  + Inbound traffic is **denied**.
  + Outbound traffic is **allowed**, except for port 25 to prevent spam.
* Example: Allowing access to a web application might require opening port 80.

**Ports**

ports are network entry and exit points through which data can travel to and from your instances. They work with security groups and network ACLs (Access Control Lists) to control traffic. Each port corresponds to a specific protocol or service.

* To get access to application know the two things they are

→ IP address

→port number

**Virtual private cloud**

The user can access the public subnet through the internet gateway

Route table

**routing** refers to directing traffic between subnets, VPCs, and external networks (like the internet or on-premises systems) using **route tables**. Each subnet in a VPC is associated with a route table, which defines the rules for where network traffic should go based on its destination IP address.

Load balancer