AWS – NAT GW, EIG, RT

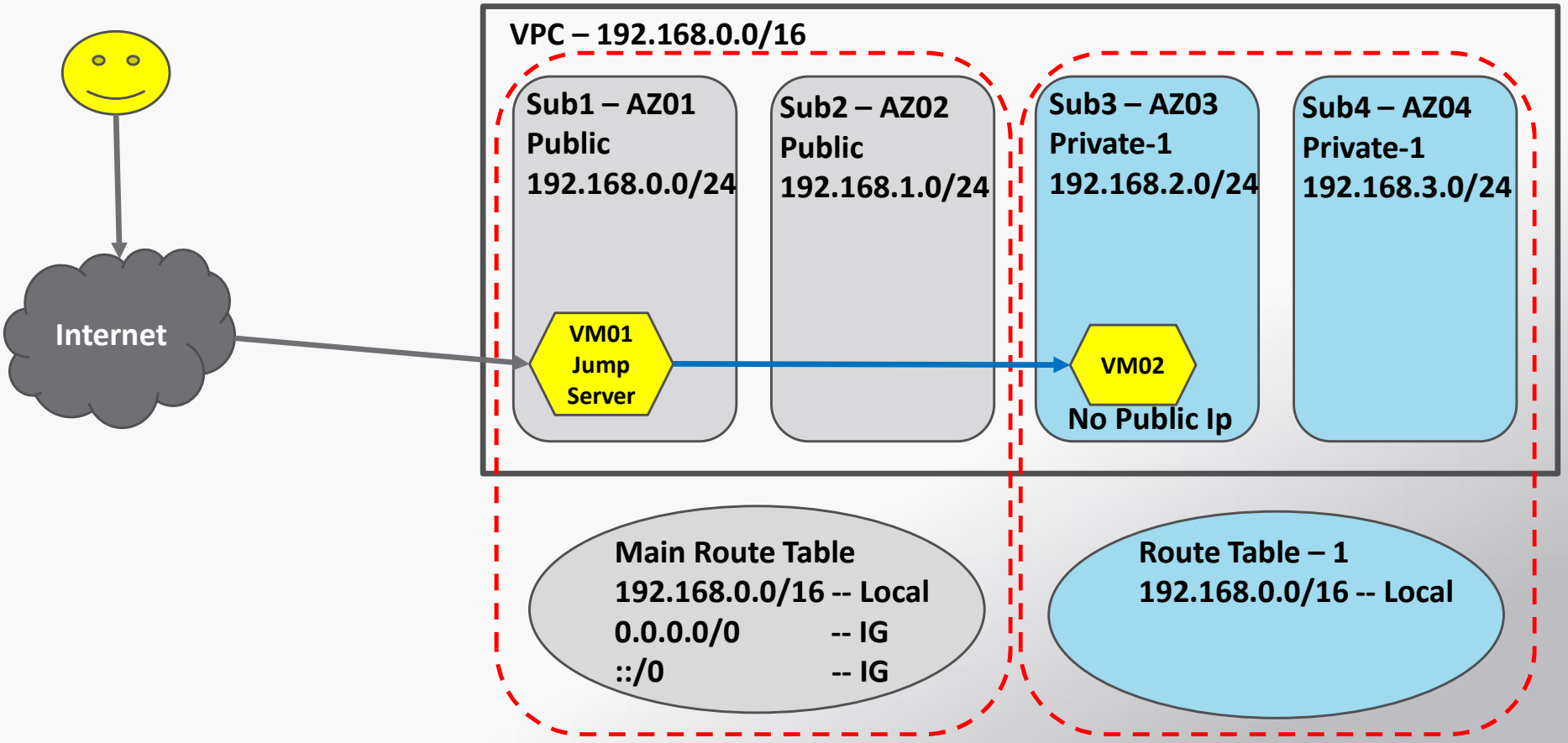
VISHWANATH M S

VISHWACLOUDLAB.COM

Creating Multiple Route Tables.

- We could have multiple Route Tables for Different Subnets in an Single VPC.
- A subnet can be part of a single Route TABLE only.

Multiple Route Table Scenario



IP Address details of EC2 (VM)

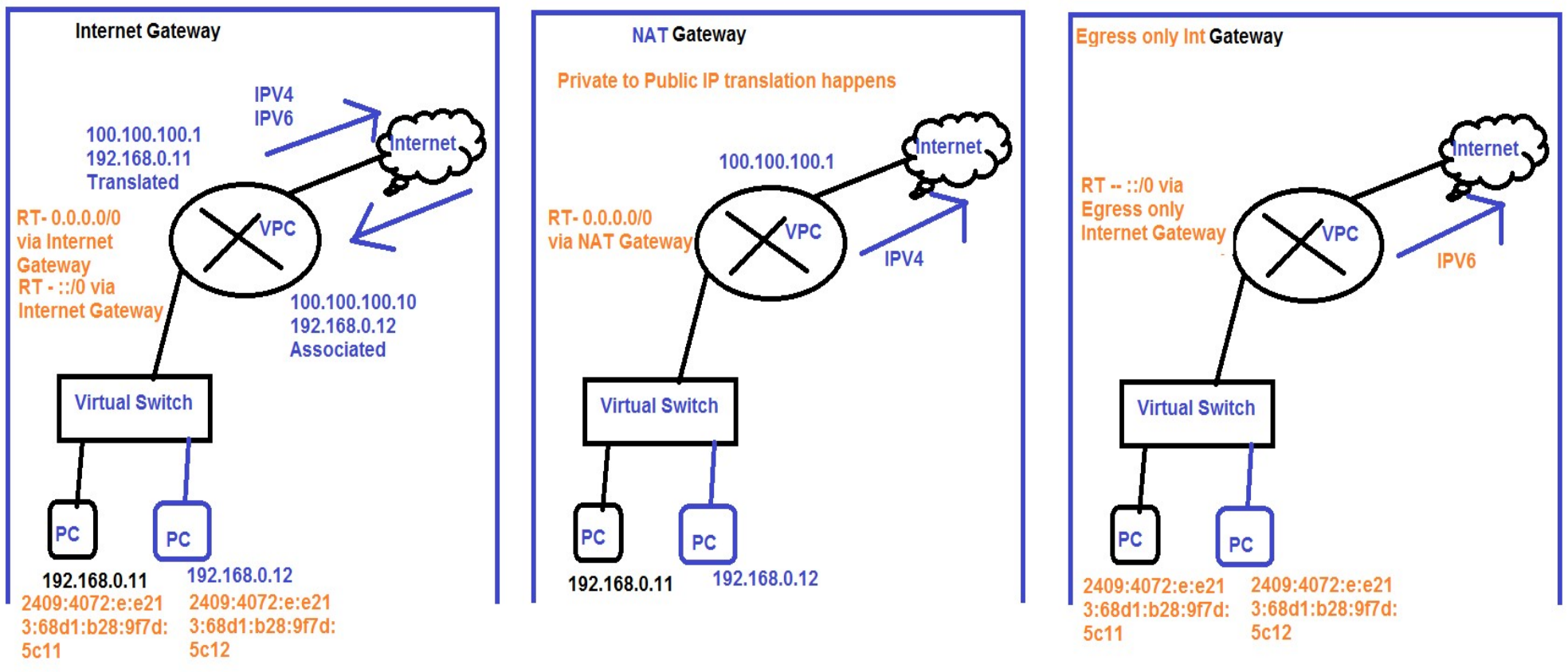
- **Private IPv4** → The assigned IPV4 to the VM is Static IP, and does not change even if the VM is shutdown or restarted and stays until the VM is "**Terminated**"
- **Public IPv4** → This is a dynamic IP **allocated** to the VM. It would change once the Vm shutdown and start back. But the IP would remain if the VM is restarted.
  - The public IPv4 is not assigned to the VM, the VPC maintains the "**NAT**" rule for private to Public mapping,
- **" Public IPv6** → This is an static IP, assigned to the VM and stays until the VM is **"terminated**

- **Static Public IPv4 –** Create an **Elastic IP and assign(Associate) the VM to public ip.**
  - This is CHARGED per Hour.

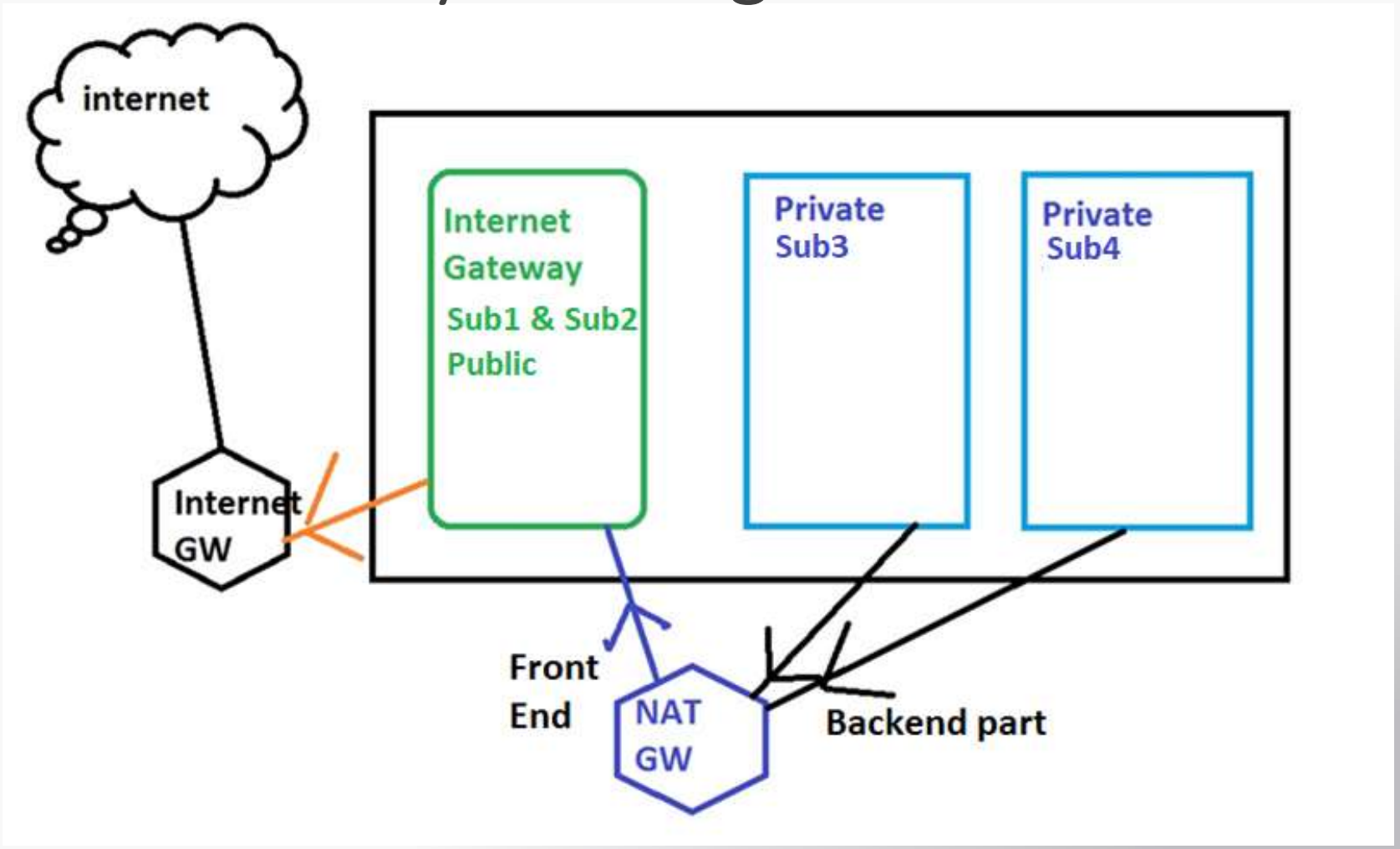
Different Gateways in VPC

- **Internet Gateway →**
  - It provides an path to the internet for the Virtual Machines in the VPC.
  - The Traffic is 2 ways, both inbound and outbound is allowed for IPv4 and IPv6.
- **Egress only Internet Gateway →**
  - It provides an path to the internet for the Virtual Machines in the VPC on IPv6 only.
  - The Traffic is **One way**, only outbound is allowed for IPv6 from the Virtual Machine.
- **NAT Gateway →**
  - It provides an path to the internet for the Virtual Machines in the VPC on **IPv4 only**.
  - The Traffic is **One way**, **only outbound is allowed** for IPv4 from the Virtual Machine.
  - There is an **Public IP assigned on the Gateway**, and there is NO USE of public ip on the Virtual machine.
  - This is NOT available for IPv6, as “NAT Gateway” is used to conserve IPv4.
  - We cannot PING any of the public ip from the VM.

Internet GW vs NAT GW vs Egress GW



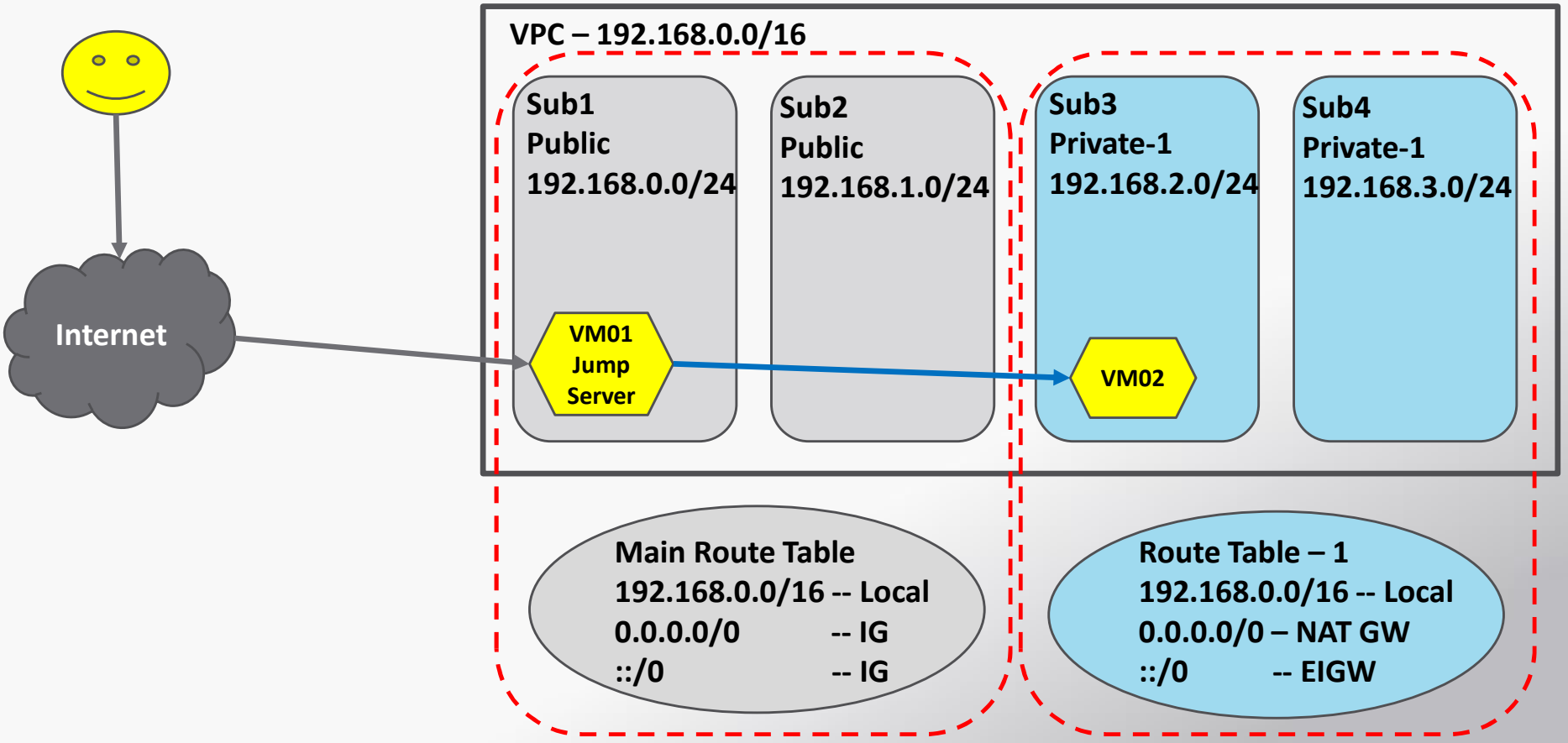
NAT Gateway Working



Steps to Create NAT Gateway

1. **Create an separate routing table for the private Subnet and associate the subnet.**
2. **Create an NAT Gateway assigning it to the Public subnet for the Internet access and assign an Elastic IP to the same**
3. **Update the custom Routing table created in Step1, with default route pointing towards NAT Gateway.**

NAT GW & EIG Scenario



PRICING

- **VPC – NOT Charged**
- **Subnets – NOT Charged**
- **Internet Gateway – NOT Charged**
- **Routing Table – NOT Charged**
- **NAT Gateway – Charged, as there is an Public IPv4 assigned to it.**
- **Egress only IG – NOT Charged**
- **VPN -- Charged, as there is an Public IPv4 assigned to it.**

Elastic IP pricing

An Elastic IP address doesn’t incur charges as long as the following conditions are true:

- The Elastic IP address is associated with an EC2 instance.
- The instance associated with the Elastic IP address is running.
- The instance has only one Elastic IP address attached to it.

You're charged by the hour for each Elastic IP address that doesn't meet these conditions.

Troubleshooting VPC

Basic Troubleshooting steps if the EC2 instance is not getting connected.

- Check Weather “Internet gateway” is created an assigned to “Routing Table”.
- If custom Route table created, weather “Subnet’s” are associated to the new Routing table.
- Weather “PORTS” are allowed in the security group for “inbound” and “outbound”.

- https://aws.amazon.com/premiumsupport/knowledge-center/troubleshoot-vpc-route-table/