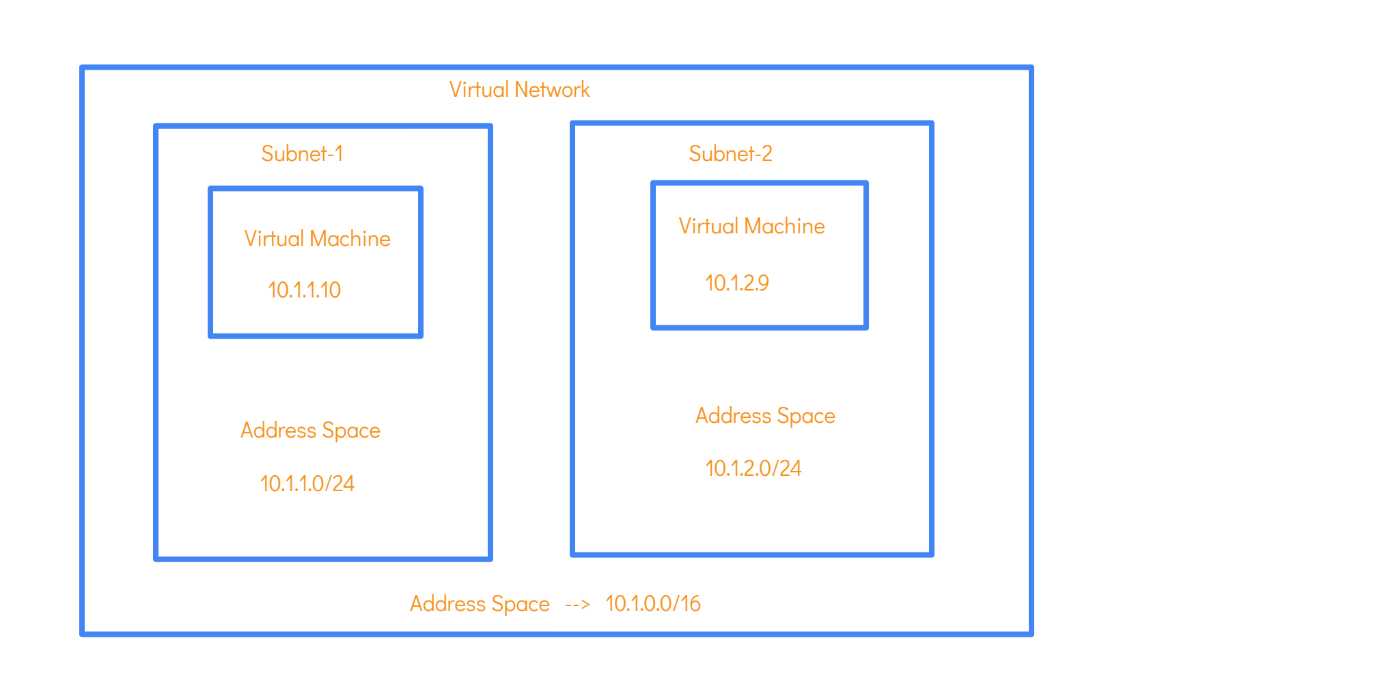
**Configuring & Managing Networking:**

**Introduction to Virtual Networks in Azure:**



* 2 VM’s in 2 different Subnet’s can communicate with each other since it’s in same V-NET.
* Subnet-1 could host webservers and Subnet-2 could host Database-servers, since it’s in same V-NET, they can communicate with each other.
* Virtual Network id scoped to a single region.

1. IP Addresses:
2. Public-IP 🡪 Used to communicate with Internet.
3. Private-IP 🡪 Used for communication within an **Azure V-Net** or with **on-premises Network**.
4. SKU’s:

There are 2 SKU’s when it comes to public IP Addresses:

1. **Basic SKU** –

* Here you can assign either static or dynamic IP Addresses.
* NSG’s can optionally be used to restricting traffic via public IP Addresses.
* There is no support for Availability zones.

1. **Standard SKU** –

* Here you can assign static IP Addresses only.
* NSG’s needs to use to restrict traffic via public IP Addresses.
* **They are zone redundant by default**. (High availability for public IP)

**Addresses Spaces:**

Address Space 🡪 10.0.0.0/24 (V-NET)

/24 🡪 Is called “**Network Prefix Length**”

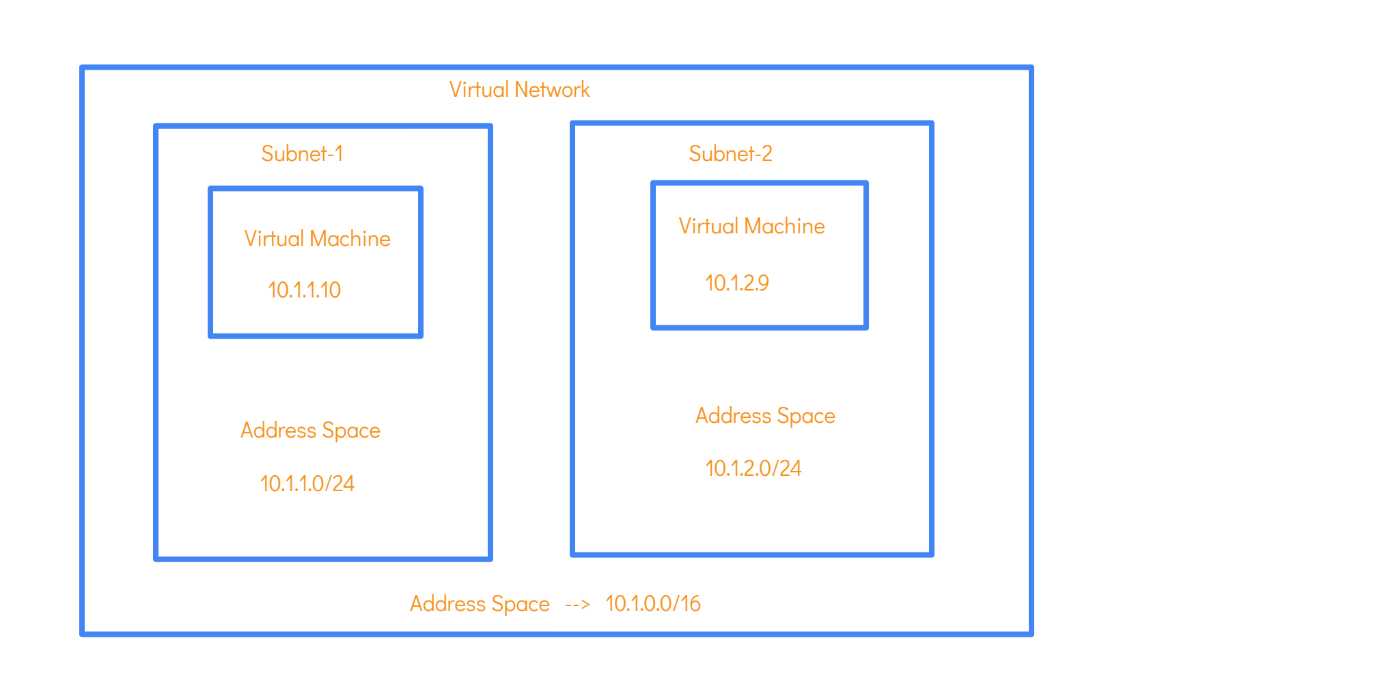
i.e., First 24 bits are already turned on and it can’t be changed.

VM 🡪 can be 10.0.0.5 (Only changing the last octet)

**Network Interface:**

* NI is a Hardware device that is available on Workstations/Laptops.
* This NI is used for the Routing of Traffic.
* Your Router will send the data you are browsing through this NI to the Internet.

When it comes to Azure if you have 2 VM’s like following:



Each of the VM has its own Network Interface with both Public and Private IP.

1. **IP’s for Network Interface of Subnet-1 (VM):**

Public-IP: 40.127.133.204 (Dynamic)

Private-IP: 10.1.1.5 (In the range of Subnet Address space)

1. **IP’s for Network Interface of Subnet-1 (VM):**

Public-IP: 20.102.123.234 (Dynamic)

Private-IP: 10.1.2.67 (In the range of Subnet Address space)

\*\*\* In the IP-Configuration section:

* You can create a Private IP for Network Interface
* You can create a Public-IP and attach the created Public-IP to this Network Interface in IP\_Configuration section.

**Attaching a Secondary Network Interface:**

**Use Case Scenario of why you need a Secondary Network Interface:**

**Network Security Groups:**

* Used to control flow of traffic Into and Out of VM. (Kind of Firewall)
* **NSG** will gets attached to the **Network Interface/Entire Subnet** that is attached to the Virtual Machine/All VM’s present in Subnet.
* There are two types of Security Rules:

1. **Inbound Security Rule –** Controls flow of traffic into the VM
2. **Outbound Security Rule –** Controls flow of traffic out from the VM

* By default, RDP port 3389 will be open while creating a VM.
* When some User/Users (Source) is trying to access the VM on port **80 (HTTP Port should be open)** on VM (Destination).