# Azure Networking

**Classless Inter-Domain Routing**

CIDR is a method for allocating and managing IP addresses efficiently.

CIDR Notation

IP address / Subnet mask

192.168.1.10/24

**Subnet Mask**

The process of dividing a network into smaller network sections is called **subnetting**.

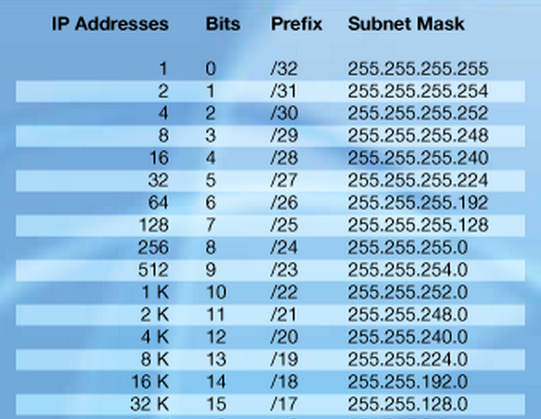
Each address space is divided into a network portion and a host portion.

A subnet mask determines which part of an IP address is network and which part is host.

**CIDR /24 means the first 24 bits are for the network, and the last 8 bits are for hosts.**

**For the address 192.168.0.15, the 192.168.0 portion describes the network and the 15 describes the host.**

**Number of IP Addresses = 2 ^(Number of Host Bits)**



**Public and Private IP**

Public networks like the Internet communicate by using public IP addresses.

Private networks like your Azure Virtual Network use private IP addresses, which aren't routable on public networks

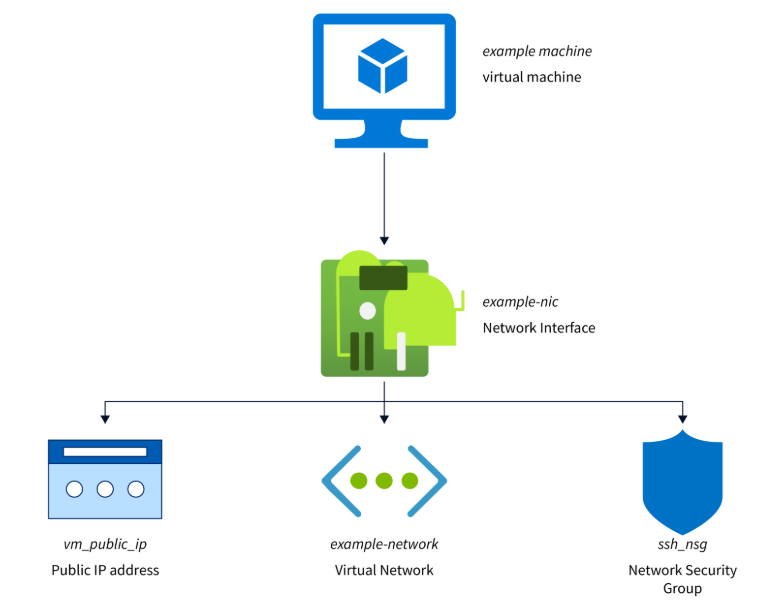
**Dynamic and Static**

Dynamic - An assigned address that can change over the lifespan of the Azure resource

Static - An assigned address that doesn't change over the lifespan of the Azure resource

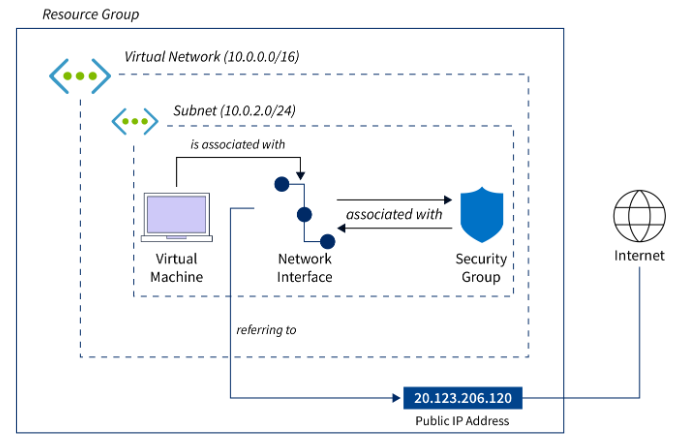
**Networking Components**

* Network Interface
* Network Security Group
* IP Address
* DNS Servers



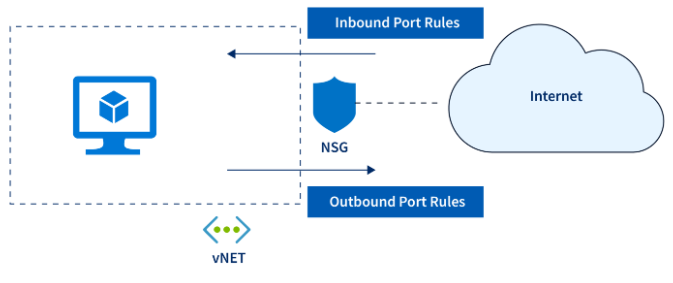
Network Interface (NIC)

* Connects a VM to a VNet.
* A gateway that allows a VM to communicate with other resources in a network.
* Manages the flow of data to and from a VM
* Each Network Interface is assigned one or more IP configurations which include ***private IP addresses, associated public IP addresses (if required), and network security group (NSG) settings.***



Network Security Group (NSG)

Acts as virtual firewalls, controlling inbound and outbound traffic to a Network Interface.



* Define inbound and outbound traffic rules.
* Filter traffic based on the source, destination, and protocol.
* Work with route tables to ensure that traffic is directed as intended.

Domain Name System (DNS) Servers

* Essential for translating human-readable domain names into IP addresses.
* Configuring DNS servers for a Network Interface ensures that it can seamlessly communicate with resources both within and outside the Azure environment.

**Demo**

**Understand Azure Network Security Groups (NSGs) and networking components.**

**AzCLI**

Create virtual network

*az network vnet create --resource-group myRGNetwork --name myVNet --address-prefix 10.0.0.0/16 --subnet-name myFrontendSubnet --subnet-prefix 10.0.1.0/24*

Create sub network

*az network vnet subnet create --resource-group myRGNetwork --vnet-name myVNet --name myBackendSubnet --address-prefix 10.0.2.0/24*

Create NSG

*az network nsg create --resource-group myRGNetwork --name myBackendNSG*

Configure NSG Rules

✅ Add Inbound Rule to Allow SSH (22)

1. Open MyNSG → Click Inbound Security Rules
2. Click Add Rule:
   * Name: Allow-SSH
   * Priority: 100
   * Source: Any
   * Destination: Any
   * Service: SSH
   * Action: Allow
3. Click Add

❌ Add Inbound Rule to Block RDP (3389)

1. Click Add Rule again:
   * Name: Block-RDP
   * Priority: 200
   * Source: Any
   * Destination: Any
   * Service: RDP
   * Action: Deny
2. Click Add

✅ Add Outbound Rule to Allow HTTP (80)

1. Go to Outbound Security Rules
2. Click Add Rule:
   * Name: Allow-HTTP-Out
   * Priority: 100
   * Destination Port Range: 80
   * Protocol: TCP
   * Action: Allow
3. Click Add

Associate NSG with a Subnet

1. Navigate to the NSG you just created.
2. Under "Settings," select "Subnets."
3. Click on "Associate" and select the virtual network and subnet you want to associate with the NSG.
4. Click "OK" to complete the association.

Configure NSG Rules

1. Navigate to the NSG you just created.
2. Under "Settings," select "Inbound security rules" or "Outbound security rules."
3. Click on "+ Add" to create a new rule.
4. Fill in the required details, such as source, destination, port, and protocol.
5. Click "Add" to create the rule.

Test Inbound

ssh azureuser@<VM\_Public\_IP> PASS

telnet <VM\_Public\_IP> 3389 FAIL

Test Outbound

curl -I http://example.com