**Private Network vs. Public Network**

1. **Private Network:**
   * A network restricted to internal devices within an organization.
   * Not accessible directly from the internet.
   * Examples: Office LANs, home Wi-Fi.
   * Common IP ranges (as per **RFC 1918**):
     + **Class A**: 10.0.0.0 – 10.255.255.255
     + **Class B**: 172.16.0.0 – 172.31.255.255
     + **Class C**: 192.168.0.0 – 192.168.255.255
2. **Public Network:**
   * A network where devices are accessible from the internet.
   * IP addresses are globally unique and allocated by **IANA** or regional registries (e.g., ARIN, RIPE).
   * Examples: Websites, cloud-hosted services.

**IP Address Classes and Subnetting Ranges**

* **Class A**:
  + Range: 0.0.0.0 – 127.255.255.255
  + Default Subnet Mask: 255.0.0.0
  + Large networks (up to ~16 million hosts).
* **Class B**:
  + Range: 128.0.0.0 – 191.255.255.255
  + Default Subnet Mask: 255.255.0.0
  + Medium networks (up to ~65,000 hosts).
* **Class C**:
  + Range: 192.0.0.0 – 223.255.255.255
  + Default Subnet Mask: 255.255.255.0
  + Small networks (up to 254 hosts).

**Subnetting** divides a network into smaller segments, optimizing IP usage and isolating traffic.

**NIC (Network Interface Card)**

* A hardware component enabling devices to connect to a network.
* Assigns the device a unique MAC address and supports communication over protocols like Ethernet, Wi-Fi, or Fiber.
* Can be physical (e.g., Ethernet card) or virtual (e.g., in virtual machines).



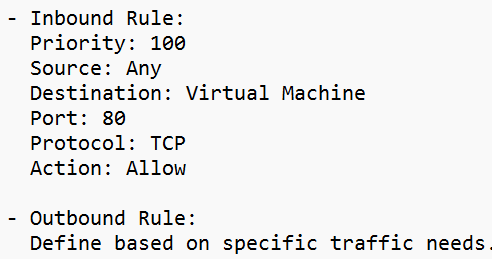
**Public IP Assignment**

* Public IPs are assigned by ISPs or cloud providers.
* In cloud platforms (e.g., AWS, Azure), public IPs:
  + Allow external access to VMs, applications, or services.
  + May be static (reserved) or dynamic (allocated temporarily).
  + Managed within a **Public IP resource** (Azure).

**NSG (Network Security Group)**

* Used in cloud platforms like Azure to control inbound and outbound traffic for resources.
* NSG rules define which traffic is allowed or denied, based on:
  + **Source/Destination IP**.
  + **Port** (e.g., 80 for HTTP, 443 for HTTPS).
  + **Protocol** (e.g., TCP/UDP).

**Example Use Case: Allow Only Port 80**



**Resource Group (Azure Concept)**

* A container for managing and organizing related Azure resources.
* Groups resources like VMs, databases, and storage accounts for easier deployment, monitoring, and cost tracking.
* Example: All resources for a web app (VM, storage, database) can reside in a single resource group.

**Service Plan (App Service Plan in Azure)**

* Defines the hosting environment for web apps, functions, and APIs.
* Determines:
  + Pricing tier (Free, Basic, Premium).
  + Compute resources (CPU, memory).
  + Scale settings (manual/auto-scale).

**Resource**

* Any manageable item in a cloud environment:
  + Examples: Virtual machines, databases, storage accounts, web apps.
* Managed through cloud platforms (e.g., Azure, AWS, GCP).

**Creating azure virtual network**

**Step 1: Log in to the Azure Portal**

1. Go to [Azure Portal](https://portal.azure.com/).
2. Log in with your Azure credentials.

**Step 2: Navigate to "Virtual Networks"**

1. In the Azure Portal search bar, type "Virtual Networks" and select it from the results.
2. Click **"Create"** or **"Add"** to start creating a new VNet.

**Step 3: Configure Basic Settings**

1. **Subscription**: Select the Azure subscription under which the VNet will be created.
2. **Resource Group**:
   * Select an existing resource group or create a new one by clicking **"Create New"**.
3. **Name**: Enter a name for your virtual network (e.g., MyVNet).
4. **Region**: Choose the region where you want the VNet to be deployed (e.g., East US).

**Step 4: Configure Address Space**

1. Click on the **"IP Addresses"** tab.
2. Define the **address space** for the VNet:
   * Use CIDR notation (e.g., 10.0.0.0/16) to specify the range of private IP addresses.
   * Ensure the address space does not overlap with other networks if you plan to connect to them.

**Step 5: Add Subnets**

1. In the **Subnets** section, click **"Add Subnet"**.
2. Define:
   * **Subnet Name**: A descriptive name (e.g., WebSubnet, AppSubnet).
   * **Subnet Address Range**: Specify the range of IPs for this subnet in CIDR format (e.g., 10.0.1.0/24).
3. Repeat for additional subnets if needed.

**Step 6: Configure Security Settings (Optional)**

1. If desired, you can configure:
   * **Network Security Groups (NSGs)**: Attach NSGs to subnets to control traffic.
   * **Firewall Settings**: Enable features like Azure Firewall for advanced security.

**Step 7: Enable DDoS Protection and Service Endpoints (Optional)**

1. Choose whether to enable **DDoS Protection** (Basic or Standard) to secure against distributed denial-of-service attacks.
2. Configure **Service Endpoints** if needed, to allow private access to Azure services (e.g., Storage, SQL).

**Step 8: Review and Create**

1. Click the **"Review + Create"** button.
2. Azure will validate your configuration. If there are errors, correct them.
3. Once validated, click **"Create"** to deploy your virtual network.

**Step 9: Verify and Use the Virtual Network**

1. Navigate to the **Virtual Networks** blade in the Azure portal.
2. Select your newly created VNet and confirm the details, including:
   * Address space.
   * Subnets.
   * Connected resources.

**Creating Azure VM within the network**

**Step 1: Log in to the Azure Portal**

1. Go to [Azure Portal](https://portal.azure.com/).
2. Log in with your Azure credentials.

**Step 2: Navigate to "Virtual Networks"**

1. In the Azure Portal search bar, type "Virtual Networks" and select it from the results.
2. Click **"Create"** or **"Add"** to start creating a new VNet.

**Step 3: Configure Basic Settings**

1. **Subscription**: Select the Azure subscription under which the VNet will be created.
2. **Resource Group**:
   * Select an existing resource group or create a new one by clicking **"Create New"**.
3. **Name**: Enter a name for your virtual network (e.g., MyVNet).
4. **Region**: Choose the region where you want the VNet to be deployed (e.g., East US).

**Step 4: Configure Address Space**

1. Click on the **"IP Addresses"** tab.
2. Define the **address space** for the VNet:
   * Use CIDR notation (e.g., 10.0.0.0/16) to specify the range of private IP addresses.
   * Ensure the address space does not overlap with other networks if you plan to connect to them.

**Step 5: Add Subnets**

1. In the **Subnets** section, click **"Add Subnet"**.
2. Define:
   * **Subnet Name**: A descriptive name (e.g., WebSubnet, AppSubnet).
   * **Subnet Address Range**: Specify the range of IPs for this subnet in CIDR format (e.g., 10.0.1.0/24).
3. Repeat for additional subnets if needed.

**Step 6: Configure Security Settings (Optional)**

1. If desired, you can configure:
   * **Network Security Groups (NSGs)**: Attach NSGs to subnets to control traffic.
   * **Firewall Settings**: Enable features like Azure Firewall for advanced security.

**Step 7: Enable DDoS Protection and Service Endpoints (Optional)**

1. Choose whether to enable **DDoS Protection** (Basic or Standard) to secure against distributed denial-of-service attacks.
2. Configure **Service Endpoints** if needed, to allow private access to Azure services (e.g., Storage, SQL).

**Step 8: Review and Create**

1. Click the **"Review + Create"** button.
2. Azure will validate your configuration. If there are errors, correct them.
3. Once validated, click **"Create"** to deploy your virtual network.

**Step 9: Verify and Use the Virtual Network**

1. Navigate to the **Virtual Networks** blade in the Azure portal.
2. Select your newly created VNet and confirm the details, including:
   * Address space.
   * Subnets.
   * Connected resources.