**What is Azure Virtual Network?**

Azure Virtual Network is a service that provides the fundamental building block for your private network in Azure. An instance of the service (a virtual network) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. These Azure resources include virtual machines (VMs).

A virtual network is similar to a traditional network that you'd operate in your own datacenter. But it brings extra benefits of the Azure infrastructure, such as scale, availability, and isolation.

## **Why use an Azure virtual network?**

Key scenarios that you can accomplish with a virtual network include:

* Communication of Azure resources with the internet.
* Communication between Azure resources.
* Communication with on-premises resources.
* Filtering of network traffic.
* Routing of network traffic.
* Integration with Azure services.

### . CIDR Range

**CIDR (Classless Inter-Domain Routing)** notation is used to specify IP address ranges for Azure VNets and subnets. Here’s what you need to know:

* **Definition:** CIDR notation combines an IP address and a prefix length (in the form of IP\_address/prefix\_length) to specify the network and subnet mask.
* **Purpose:** CIDR helps in efficiently allocating IP addresses and defining the size of subnets within a VNet.
* **Considerations:** When choosing a CIDR range, consider the number of resources (like VMs) you plan to deploy within the VNet and how you want to segment your network for security and management purposes.
* **Example:** If you choose a CIDR block of 10.0.0.0/16 for your VNet, it allows for up to 65,536 IP addresses.

### 2. Subnetting

**Subnetting** involves dividing a larger network (VNet) into smaller sub-networks (subnets):

* **Purpose:** Subnetting allows you to logically segment your VNet to improve network management, security, and resource utilization.
* **Guidelines:** Decide on the number of subnets needed based on your application requirements (e.g., front-end, back-end, management) and distribute IP addresses accordingly.
* **Configuration:** Within Azure Portal, you can create subnets under your VNet, each with its own CIDR block, to organize resources and apply network security policies.

### 3. VNet Peering

**VNet Peering** allows connecting Azure VNets within the same region:

* **Definition:** VNet peering enables seamless connectivity between Azure VNets. It allows resources in different VNets to communicate securely as if they are on the same network.
* **Types:** There are two types of VNet peering: **same-region peering** (within the same Azure region) and **global peering** (across Azure regions, but with some limitations).
* **Use Cases:** Use VNet peering to integrate multi-tier applications spread across different VNets, consolidate management and monitoring, and reduce data transfer costs between VNets.

### 4. Windows and Linux Virtual Machines

Deploying **Windows and Linux VMs** within an Azure VNet involves several considerations:

* **VM Deployment:** Azure provides a wide range of VM sizes and OS images (Windows Server, Ubuntu, CentOS, etc.) to choose from based on your workload requirements.
* **Networking:** When deploying VMs, you can assign them to specific subnets within your VNet to control network traffic and apply network security groups (NSGs) for firewall rules.
* **Availability:** Utilize availability sets or availability zones to ensure high availability and resilience of VMs against datacenter failures.
* **Integration:** Integrate VMs with other Azure services within the VNet, such as Azure SQL Database or Azure Storage, to build scalable and reliable applications.

### Prerequisites for Creating an Azure Virtual Network (VNet)

**1. Azure Subscription and Access:**

* **Azure Subscription:** You need an active Azure subscription. If you don't have one, you can sign up for a free Azure account which provides you with a $200 credit to explore Azure services for the first 30 days.
* **Azure Portal Access:** Ensure you have access to the Azure portal (portal.azure.com) with appropriate permissions to create and manage resources.

**2. Understanding CIDR Notation:**

* **CIDR (Classless Inter-Domain Routing):** It's crucial to understand how CIDR notation works as it is used to specify IP address ranges for Azure VNets and subnets. CIDR notation consists of an IP address followed by a slash (/) and a number indicating the network prefix length.

**3. Networking Concepts:**

* **IP Addressing and Subnetting:** Familiarize yourself with IP addressing concepts, subnetting, and how these concepts apply to Azure VNets. Understand how to calculate subnet sizes and how to reserve IP address ranges.
* **DNS (Domain Name System):** Understand DNS resolution in Azure and how DNS settings are configured within a VNet.

**4. Azure Resource Groups:**

* **Resource Groups:** Azure VNets are created within Azure Resource Groups. Understand the concept of resource groups, their purpose in organizing and managing Azure resources, and how to create and manage them.

**5. Planning for Connectivity:**

* **Internet Connectivity:** Decide whether your VNets need to be connected to the internet directly or through Azure services like Azure Firewall or Network Virtual Appliances (NVAs).
* **Hybrid Connectivity:** Understand options for connecting Azure VNets to on-premises networks, such as using VPN Gateway or Azure ExpressRoute.

**6. Azure Active Directory Integration (Optional):**

* **Azure AD Integration:** If your organization uses Azure Active Directory, understand how to integrate Azure VNets with Azure AD for identity and access management.

**7. Security Considerations:**

* **Network Security Groups (NSGs):** Understand NSGs and how they are used to filter inbound and outbound traffic to and from Azure resources within a VNet.
* **Firewall Rules:** Plan and configure firewall rules to control traffic flow within the VNet and between VNets if VNet peering is utilized.

**8. Resource Naming and Tagging Standards:**

* **Naming Conventions:** Establish naming conventions for resources within Azure VNets and adhere to Azure's naming guidelines to maintain consistency and manageability.
* **Resource Tagging:** Utilize resource tagging to categorize and manage resources effectively, especially if managing multiple VNets or complex environments.

**9. Compliance and Governance Requirements:**

* **Compliance:** Ensure your VNet configurations meet any regulatory compliance requirements relevant to your organization or industry.
* **Governance:** Implement Azure policies and management groups to enforce organizational standards and compliance across VNets.

**10. Monitoring and Management:**

* **Monitoring:** Plan for monitoring network traffic, performance metrics, and logging within Azure VNets using Azure Monitor or third-party tools.
* **Management Tools:** Familiarize yourself with Azure networking tools and APIs for managing and automating VNet configurations.

### Next Steps

After gathering these prerequisites, you'll be well-prepared to start designing and implementing Azure Virtual Networks according to your organization's requirements. Ensure to document your decisions and configurations to facilitate future management and troubleshooting.

By addressing these prerequisites, you'll have a solid foundation to create Azure VNets efficiently and securely, leveraging Azure's robust networking capabilities to meet your business needs.

**Conclusion: Research and Development on Azure Virtual Network**

In conclusion, conducting research and development (R&D) on Azure Virtual Network (VNet) involves gathering essential prerequisites to ensure a successful deployment and management of network resources within Azure.

**Understanding Azure Virtual Network (VNet):** Azure VNets serve as the cornerstone for connecting and isolating Azure resources securely. They provide network segmentation, control over traffic flow, and integration capabilities with on-premises networks and Azure services.

**CIDR Range and Subnetting:** CIDR notation is crucial for defining IP address ranges for VNets and subnets. Proper planning ensures efficient allocation of IP addresses and facilitates subnetting to organize resources based on functional requirements such as application tiers or security zones.

 **VNet Peering:** VNet peering enables seamless connectivity between VNets within the same Azure region, allowing resources to communicate securely without needing a gateway or traversing the internet. Understanding different peering scenarios and their limitations helps in designing scalable and resilient network architectures.

 **Deployment of Windows and Linux Virtual Machines:** Azure offers a wide range of VM sizes and operating system images to meet diverse workload requirements. Integrating VMs into VNets involves assigning them to appropriate subnets, configuring network security groups (NSGs) for traffic control, and ensuring connectivity to other Azure services and on-premises environments as needed.

 **Prerequisites and Considerations:** Before creating an Azure VNet, ensure you have:

* **Azure Subscription and Access:** An active Azure subscription with appropriate permissions.
* **CIDR Notation Understanding:** Familiarity with CIDR for IP address range allocation.
* **Network Planning:** Considerations for subnetting, connectivity requirements (internet, hybrid, VNet peering), and security (NSGs, firewall rules).
* **Resource Organization:** Establish naming conventions, tagging standards, and compliance requirements to streamline management and governance.

 **Next Steps:** After gathering prerequisites, proceed with:

* **Creating Azure Virtual Networks:** Using Azure Portal or Infrastructure as Code (IaC) tools like Azure Resource Manager (ARM) templates or Terraform.
* **Configuring Subnets and Peering:** Define CIDR ranges, create subnets, and establish VNet peering relationships to enable seamless communication between VNets.
* **Deploying Virtual Machines:** Choose appropriate VM sizes and OS images, configure networking settings within VNets, and optimize for performance and cost efficiency.