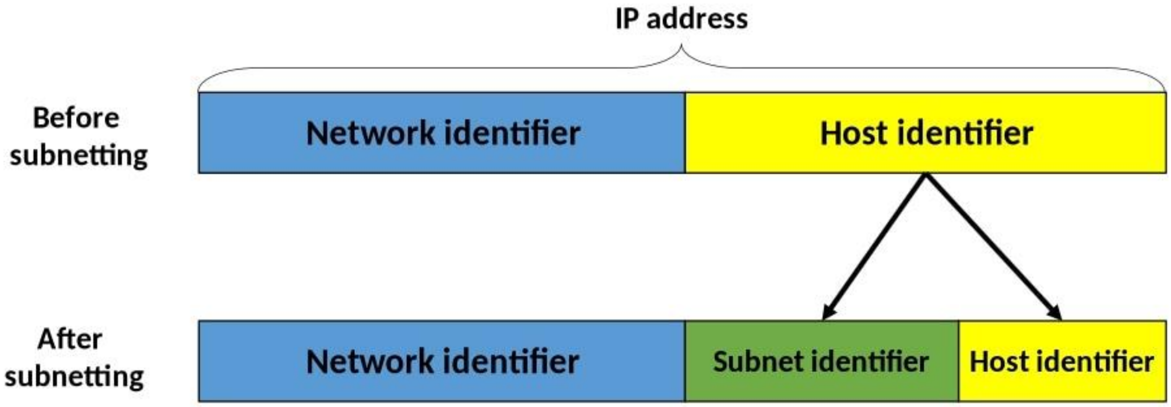
Virtual Networks In Microsoft Azure: VNet Peering

Understanding networking is a fundamental part of configuring complex environments on the internet. This has implications when trying to communicate between servers efficiently, developing secure network policies, and keeping your nodes organized.

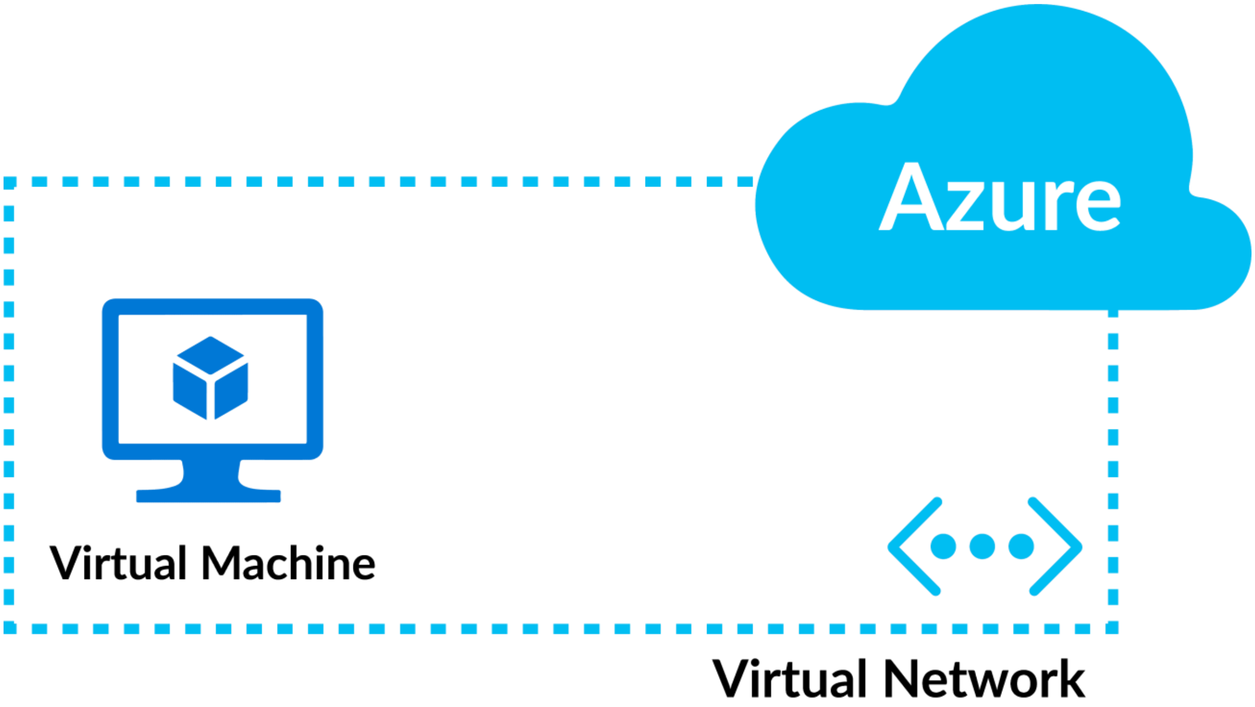
Subnetting is the process of stealing bits from the HOST part of an IP address in order to divide the larger network into smaller sub-networks called **subnets.**



CIDR or Classless Inter-Domain Routing provides the flexibility of borrowing bits of the Host part of the IP address and using them as Network in Network, called **Subnet.** By using subnetting, one single Class IP address can be used to have smaller sub-networks which provides better network management capabilities.

What Is Virtual Network?

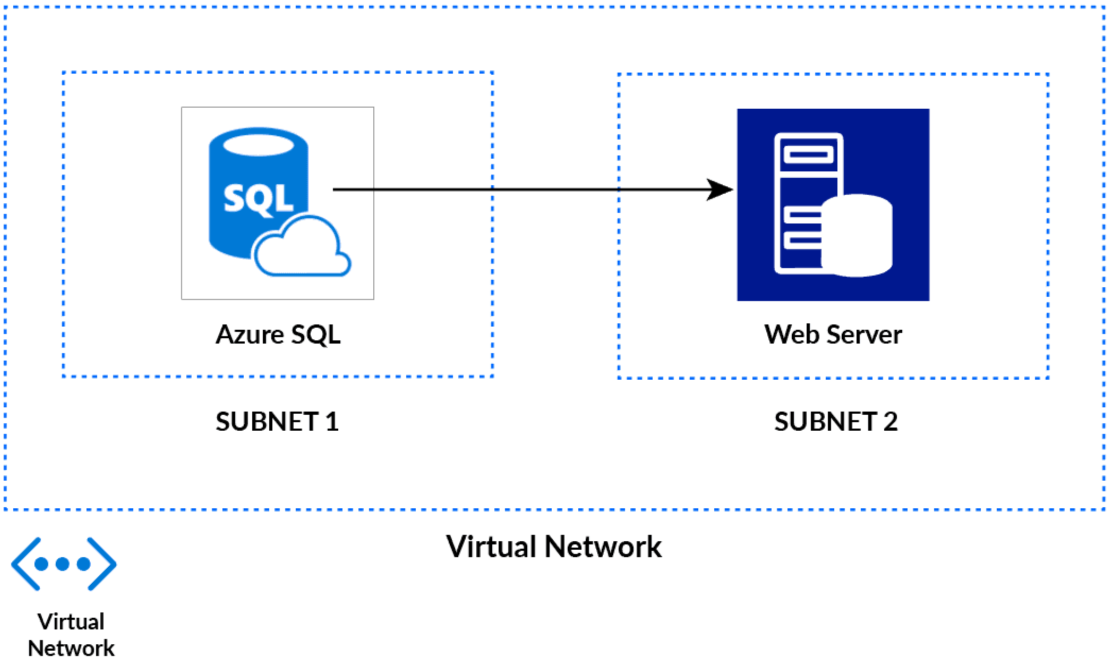
- **Azure Virtual Network (VNet)** is the fundamental building block for your private network in Azure.
- It enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely **communicate with each other, the internet**, and **on-premises networks.**
- It is similar to a traditional network that you'd operate in your own data center but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.



Use of Virtual Network?

The main purpose of Virtual Networks is to act as a communication channel between resources launched in the cloud. Why Virtual? Because there are no actual routers or switches in the cloud.

For example, if you launch a database server and a website server in the cloud, they would need a medium to interact. This medium of interaction is called a **Virtual Network.**

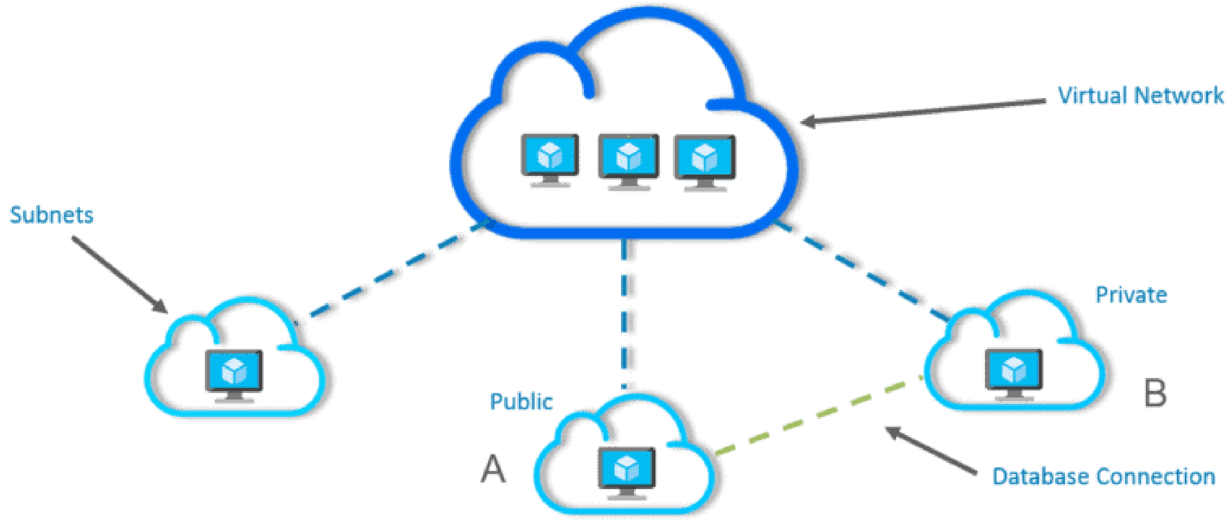


Virtual Network Key Components

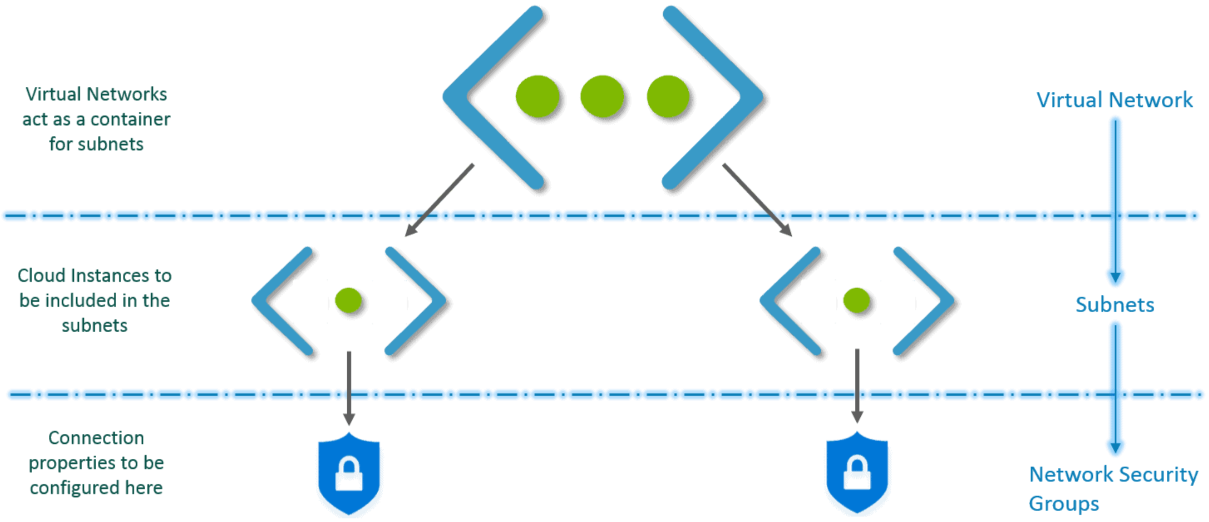
Key components of Azure VNets, include:

1**. Subnets:** Subnets enable segmenting a virtual network into one or more subnet networks and allocating a portion of the virtual network addresses space to each subnet. Azure resources are deployed to a specific subnet that is segmented using VNet address space. A subnet can further be divided into:

- **Private Subnet** – A network in which there is no internet access.
- **Public Subnet** – A network in which there is internet access.



2. **Network Security Groups (NSG):** Use to permit or deny traffic (inbound or outbound), via rules, to a subnet or network interface.
Any Azure virtual network can be placed into a security group where different inbound and outbound rules can be configured to allow or deny certain types of traffic. For each rule, you can specify source and destination, port, and protocol.


Virtual Networks act as a container for subnets
Virtual Network
Cloud Instances to be included in the subnets
Subnets
Connection properties to be configured here
Network Security Groups

How Does it Work?

- First, you create a **virtual network.**
- Then, in this virtual network, you create **subnets**.
- You associate each subnet with the respective **Virtual Machines** or Cloud Instances.
- Attach the relevant **Network Security Group** to each subnet.

- Configure the properties in the NSGs and you are set

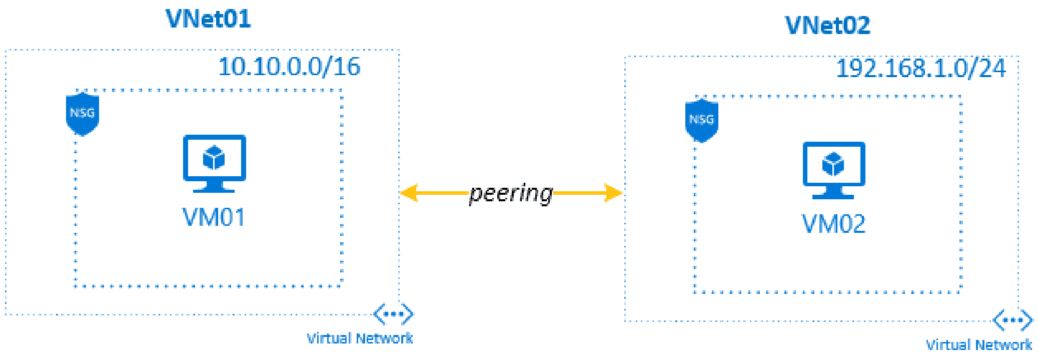
VNet Peering (Connection Between Azure VNets):

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's *private* network only.
VNet peering doesn't use a VPN gateway and has different constraints. Additionally, VNet peering pricing is calculated differently than VNet-to-VNet VPN Gateway pricing.

Azure supports the following types of peering:

Azure supports the following types of peering:

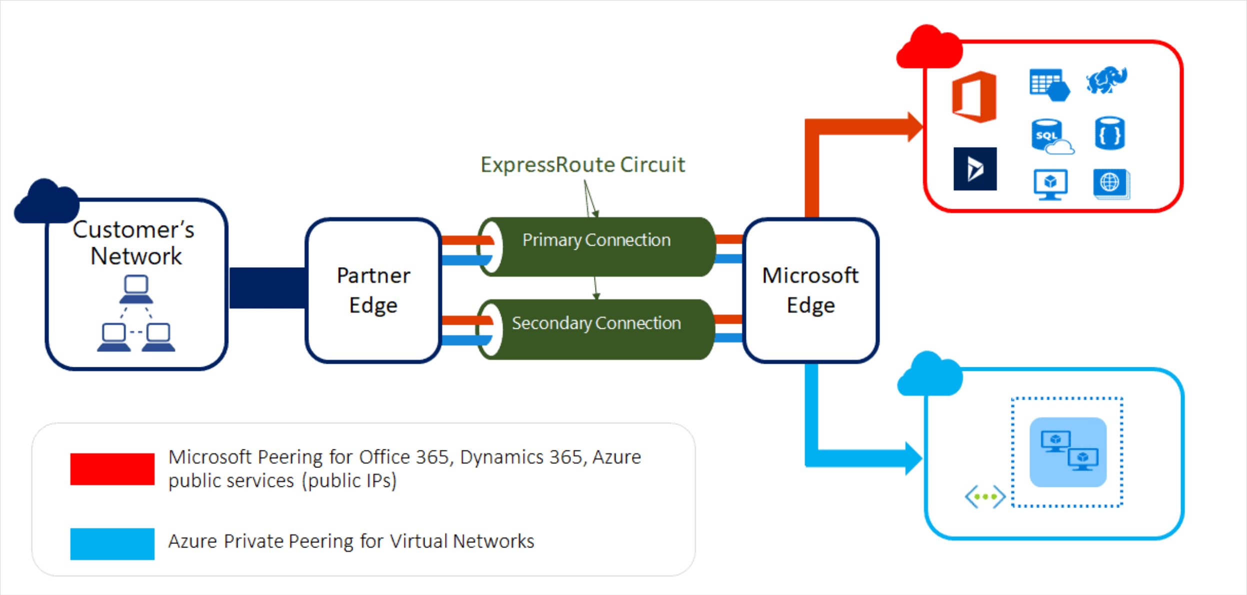
- **Virtual network peering:** Connect virtual networks within the same Azure region.
- **Global virtual network peering:** Connecting virtual networks across Azure regions.



ExpressRoute (Connection Between On-prem to Azure):

ExpressRoute is an Azure networking service that privately connects (connections don't go over the public Internet) an enterprise's on-premises infrastructure to the Microsoft public cloud via a third-party connectivity provider. Because the connection is private, it offers lower latency and greater reliability than the public internet. Azure ExpressRoute connectivity providers include Comcast, AT&T and Equinix.

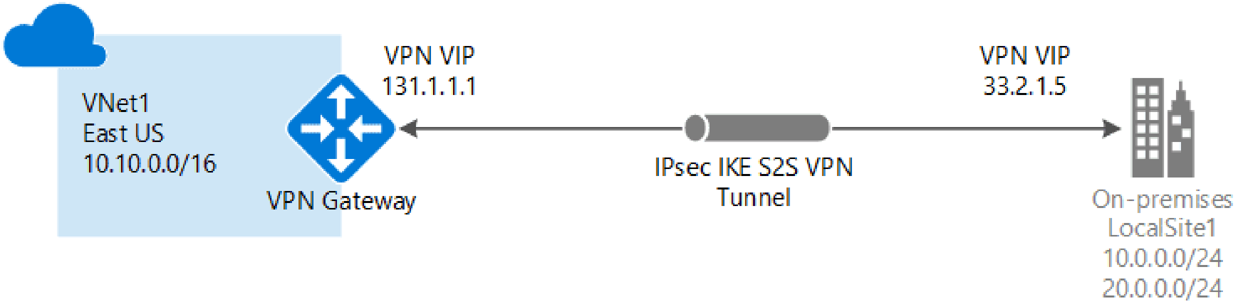
With **ExpressRoute**, you can establish connections to Microsoft cloud services, such as **Microsoft Azure**, **Microsoft 365**, and **Dynamics 365.**


ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
Azure Private Peering for Virtual Networks

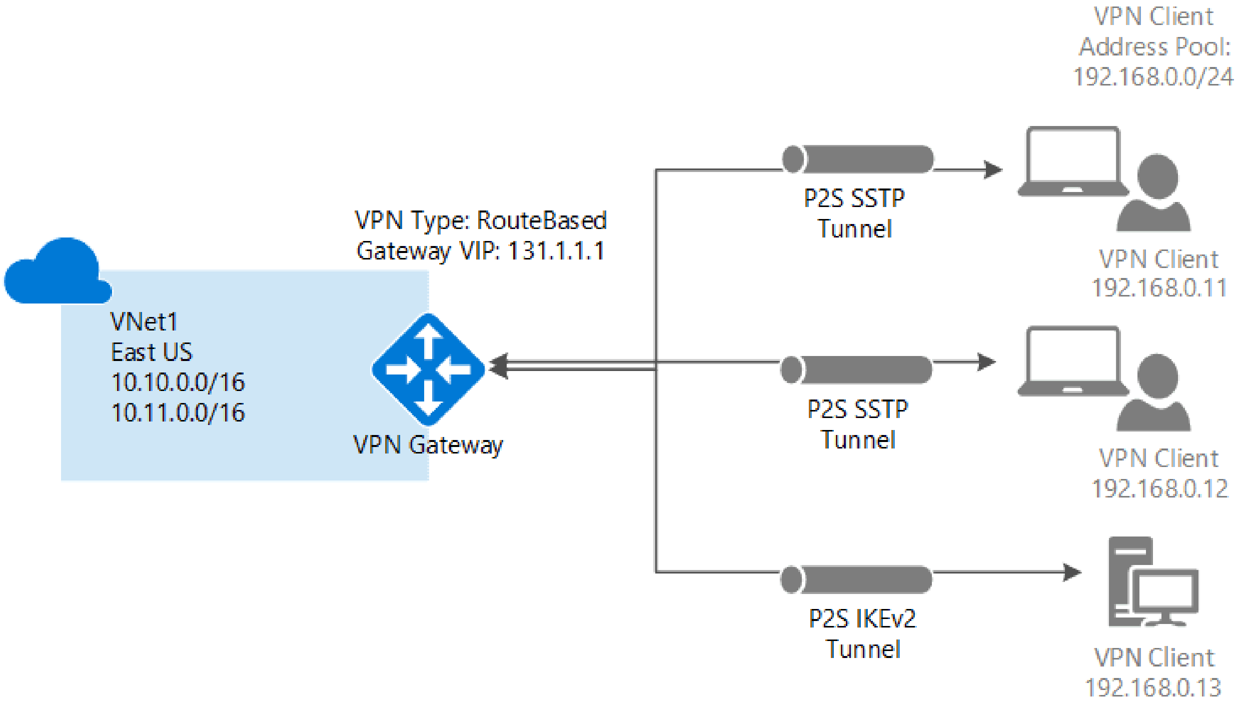
VPN Gateway (For Encrypted Connections):

VPN Gateway helps you create encrypted cross-premises connections to your virtual network from on-premises locations, or create encrypted connections between VNets. It is composed of two or more VMs that are deployed to a specific subnet you create called the ***gateway subnet.***
There are three different configurations available for VPN Gateway connections:

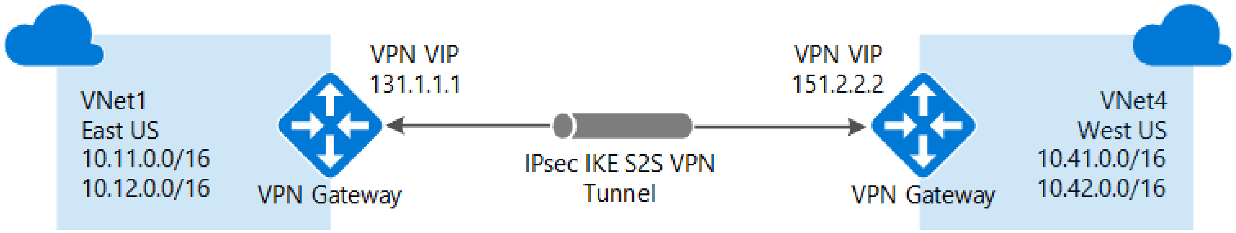
1. Site-to-Site (S2S): A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over a VPN (Virtual Private Network) tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.
Also, when you follow the Site-to-Site IPsec steps, you create and configure the local network gateways (a specific object that represents your on-premises location (the site) for routing purposes) manually. The local network gateway for each VNet treats the other VNet as a local site.



2. Point-to-Site (P2S): A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference



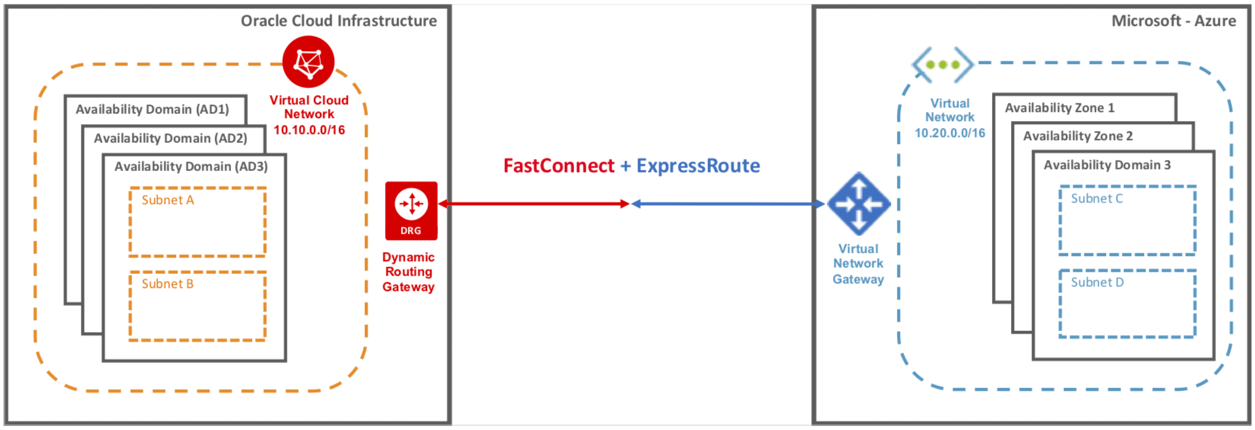
3. VNet-to-VNet: When you connect a virtual network to another virtual network with a VNet-to-VNet connection type (VNet2VNet), it's similar to creating a Site-to-Site IPsec connection to an on-premises location. Both connection types use a VPN gateway to provide a secure tunnel with IPsec/IKE and function the same way when communicating. However, they differ in the way the local network gateway is configured.
When you create a VNet-to-VNet connection, the local network gateway address space is automatically created and populated.



Interconnection between Azure and Oracle Cloud:

Microsoft and **Oracle** offer direct interconnection between Azure and Oracle Cloud Infrastructure (OCI) through **ExpressRoute** and **FastConnect.** Through the ExpressRoute and FastConnect interconnection, customers can experience low latency, high throughput, private direct connectivity between the two clouds.

Using this cross-cloud connectivity, you can partition a multi-tier application to run your database tier on Oracle Cloud Infrastructure (OCI), and the application and other tiers on Microsoft Azure. The experience is similar to running the entire solution stack in a single cloud.

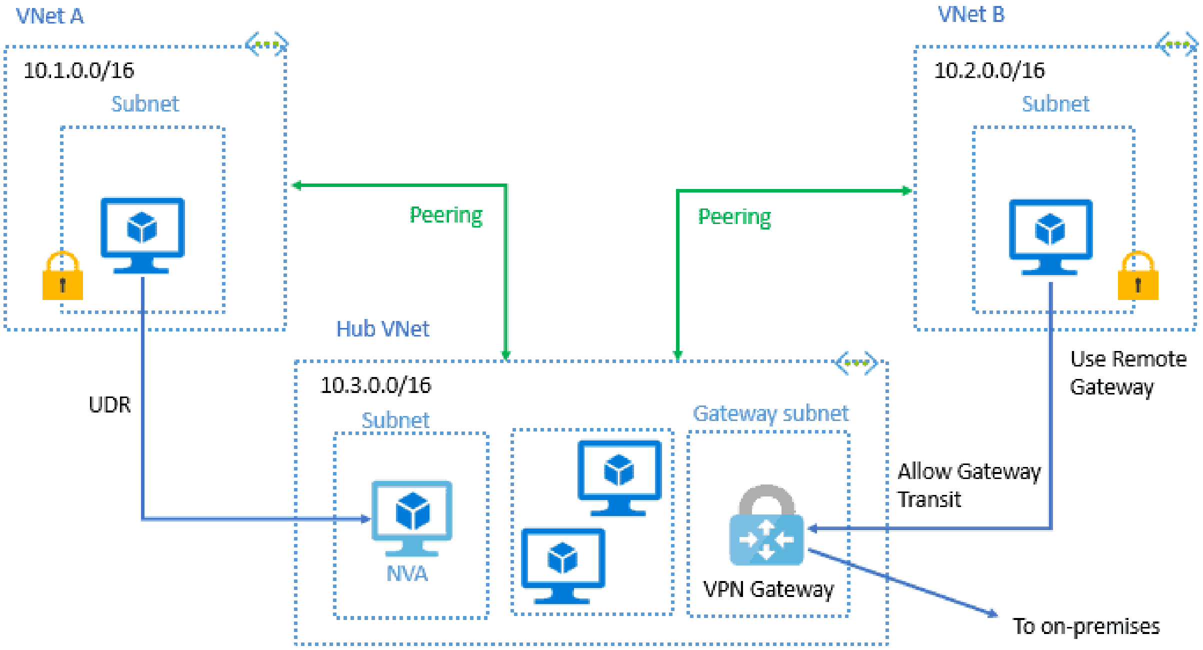


Pricing of Virtual Networks

There is **no charge** for using Azure VNet, it is free of cost.

- Standard charges are applicable for resources, such as Virtual Machines (VMs) and other products.
- You are charged for the **public IP address** and **reserved IP address** inside your VNet.
- The incoming and outgoing data of VNet Peering is chargeable.
- Also, you can calculate the resources price using the Azure pricing calculator.

A virtual network is a network of IP addresses in a range connected together. It is an important aspect of consideration while designing solutions in the cloud. In order to secure each layer of application architecture inside a highly secured network, it is recommended to create different subnets for different tiers of an application and attach each subnet with a network security group with limited inbound and outbound security rules.


VNet A
10.1.0.0/16
Subnet
Peering
Peering
VNet B
10.2.0.0/16
Subnet
Hub VNet
Use Remote Gateway
UDR
10.3.0.0/16
Subnet
Gateway subnet
Allow Gateway Transit
NVA
VPN Gateway
To on-premises