VIRTUAL NETWORKS & MACHINES

CIDR Ranges in Azure Virtual Networks (VNet):

CIDR, or Classless Inter-Domain Routing, is a standardized method for allocating IP addresses and routing IP packets. It's a highly flexible and efficient way to manage IP address space compared to older, less efficient class-based addressing systems.

When you create an Azure VNet, you must define its overall IP address space using one or more CIDR blocks. This address space acts as the boundary for all the private IP addresses that your resources within this VNet can use.

Resource IP Allocation: Every Azure resource that you deploy into this VNet will be assigned a private IP address from this defined address space.
Non-Overlapping Requirement: It is absolutely critical that the CIDR range you assign to your VNet do not overlap with any other networks you plan to connect to.

The RFC 1918 document defines these specific blocks of IP addresses that are set aside for private use:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

By using IP addresses from these ranges for Azure VNets and their subnets, you guarantee that your internal network traffic stays private and doesn't interfere with anything on the public internet. It provides a layer of isolation and security for your cloud infrastructure.

Subnets in Azure Virtual Networks (VNet):

A subnet is a logical division of an IP network. In Azure, a subnet is a range of IP addresses carved out from your VNet's larger address space. Every Azure resource that requires network connectivity (like a Virtual Machine, a database instance, or a container service) must be deployed into a specific subnet within a VNet.

Why Use Subnets?

- Logical Segmentation
- Enhanced Security
- Improved Performance and Management

If your VNet has an overall address space of 10.0.0.0/16 (which provides 65,536 available IP addresses, ranging from 10.0.0.0 to 10.0.255.255), you could then define subnets within this range, such as:

- 10.0.1.0/24 (256 addresses) for your web servers.
- 10.0.2.0/24 (256 addresses) for your application servers.
- 10.0.3.0/24 (256 addresses) for your database servers.
- Each of these subnets is "carved out" from the larger 10.0.0.0/16 space, and their IP ranges do not overlap with each other within the VNet.

Reserved IP Addresses in Subnets:

Azure reserves 5 IP addresses within each subnet's CIDR range. These addresses are automatically used by Azure for network functions and cannot be assigned to your VMs or other resources.

- 192.168.1.0 : Network address
- 192.168.1.1 : Reserved by Azure for the default gateway
- 192.168.1.2, 192.168.1.3 : Reserved by Azure to map the Azure DNS IPs to the VNet space
- 192.168.1.255 : Network broadcast address.

VNet Peering and Its Types :

As your cloud environment grows, you may find yourself with multiple Azure Virtual Networks (VNets) that need to communicate with each other. While subnets provide segmentation within a VNet, VNet Peering provides a seamless and secure way to connect different VNets, making them appear as a single, unified network for connectivity purposes.

What is VNet Peering?

VNet Peering is a mechanism in Azure that allows you to directly connect two or more Virtual Networks. Once peered, resources (like Virtual Machines) in one VNet can communicate with resources in the other peered VNet using private IP addresses, as if they were part of the same network.

Types of VNet Peering:

Azure supports two primary types of VNet peering, based on the location of the virtual networks:

- **Virtual Network Peering:**

Connects VNets that are in the same Azure region (e.g., both in "Central India").

Benefit: This is the fastest and lowest latency connection because the traffic stays entirely within that single Azure datacenter region.

- **Global Virtual Network Peering:**

Connects VNets that are in different Azure regions (e.g., one in "East US" and another in "West Europe").

Benefit: Allows you to connect your cloud services across geographical distances securely and efficiently, great for disaster recovery or applications with users worldwide.

CONCLUSION

In summary, a strong Azure network relies on these core components:

- **Azure Virtual Network (VNet)**: Your private cloud network; its size is defined by CIDR ranges for IP address allocation.
- **Subnets**: Smaller, logical segments within your VNet's CIDR range, used for organizing resources and delegating services (5 IPs reserved per subnet).
- **VNet Peering**: Creates direct, private, high-performance connections between separate VNets, avoiding the public internet.
- **Types of Peering:**
- Regional Peering: Connects VNets within the same Azure region.
- Global Peering: Connects VNets across different Azure regions.

Submitted by:
Sambit Kumar Panda

References:

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview