Research Development Document

Azure Virtual Network: CIDR, Subnets, VNet Peering

Tushar Bhosale

June 22, 2025

Contents

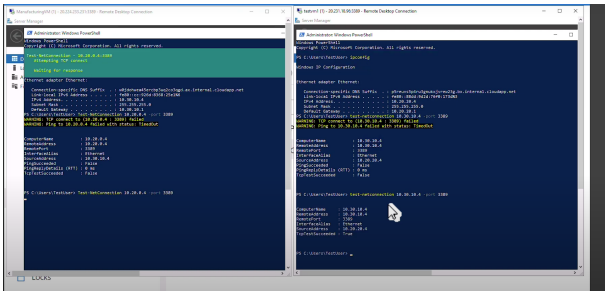


Figure 1: Enter Caption

1 Introduction

Azure Virtual Network (VNet) is the fundamental building block for private network communication in Azure. It enables resources such as virtual machines (VMs) to securely communicate with each other, the internet, and on-premises networks.

2 CIDR Ranges in Azure

CIDR (Classless Inter-Domain Routing) is used in Azure to define the IP address space of VNets and Subnets.

2.1 CIDR Range for VNet

- Defines the overall IP range allocated to a VNet. - Example: 10.0.0.0/16 allows up to 65,536 addresses.

2.2 CIDR Range for Subnet

- Each subnet is a subset of the VNet CIDR. - Example: 10.0.1.0/24 supports 256 addresses. - Subnets divide a VNet to isolate workloads logically.

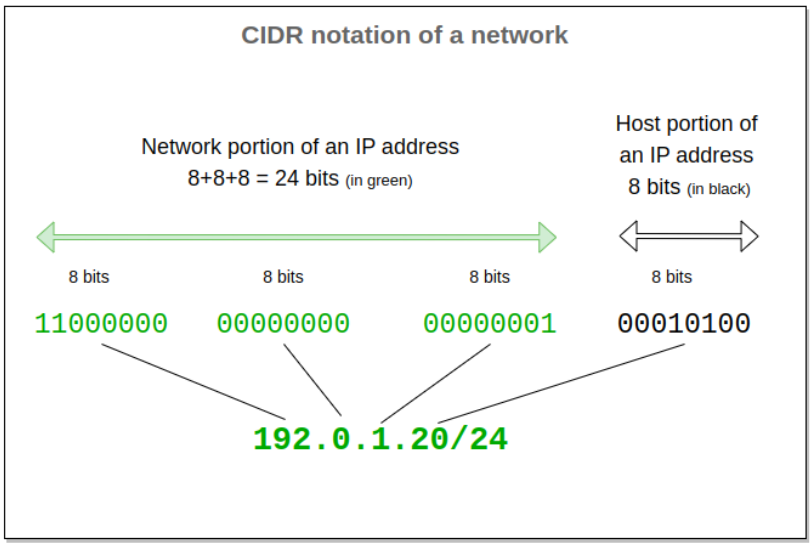


Figure 5: CIDR Division of a VNet into Subnets

3 Azure Virtual Network Prerequisites

Before creating a VNet, ensure:

- Azure subscription
- Resource Group availability
- Region selection

- CIDR planning (avoid overlaps for peering)
- Security groups and firewall rules are configured

4 VNet Peering

VNet peering allows direct connectivity between two Azure virtual networks.

4.1 Types of Peering

- **Intra-region Peering:** Between VNets in the same region.
- **Global Peering:** Between VNets in different Azure regions.

4.2 Peering Considerations

- Peered VNets must not have overlapping IP ranges.
- Peering is non-transitive.
- Can enable/disable traffic forwarding and gateway sharing.

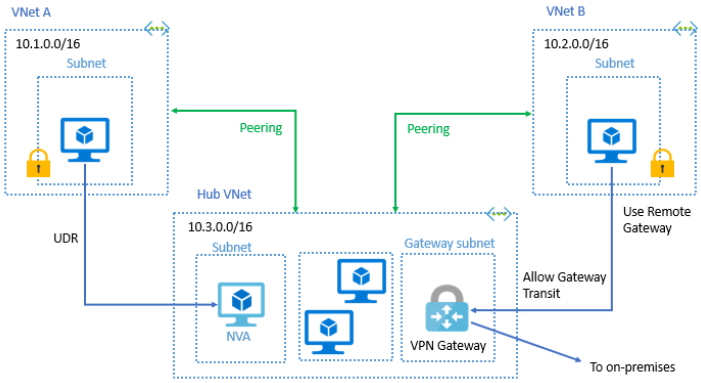


Figure 6: Types of VNet Peering

5 Use Case: Creating VNets, Subnets, and Peering

5.1 Goal

Create:

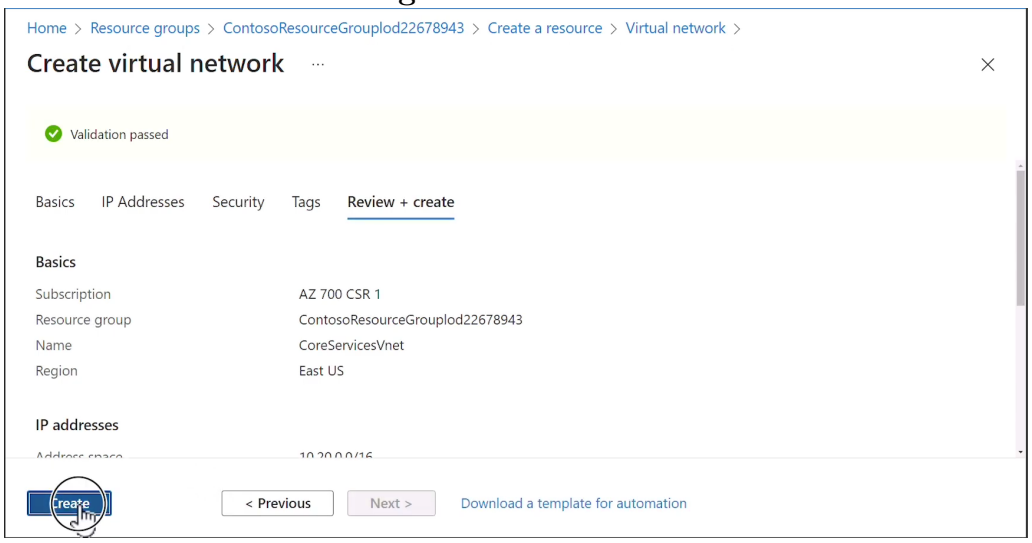
- VNet1 with Subnet1 (for Windows VM)
- VNet2 with Subnet2 (for Linux VM)
- Enable communication using VNet Peering

5.2 Step-by-Step Configuration

5.2.1 Step 1: Create VNet1

- CIDR: 10.0.0.0/16
- Subnet1: 10.0.1.0/24

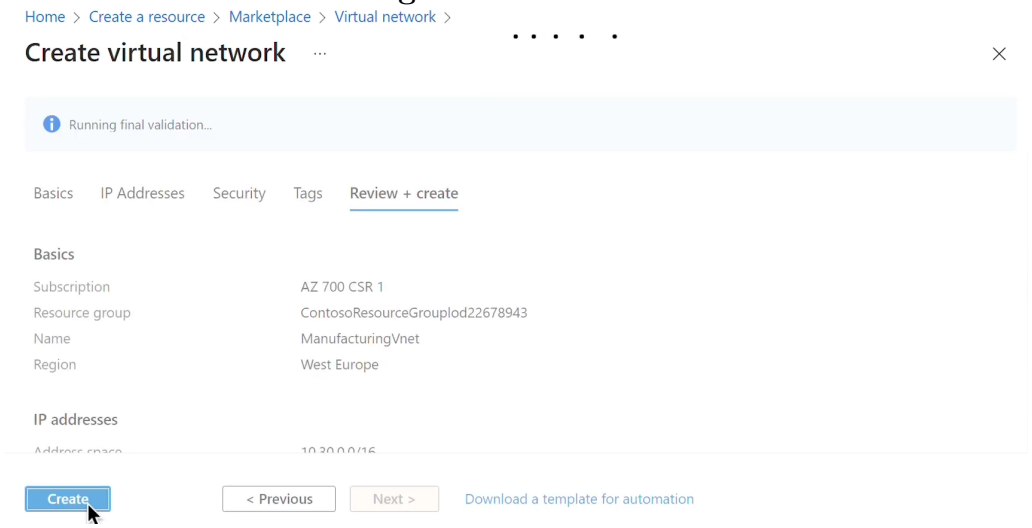
Screenshot: VNet1 Configuration



5.2.2 Step 2: Create VNet2

- CIDR: 10.1.0.0/16
- Subnet2: 10.1.1.0/24

Screenshot: VNet2 Configuration



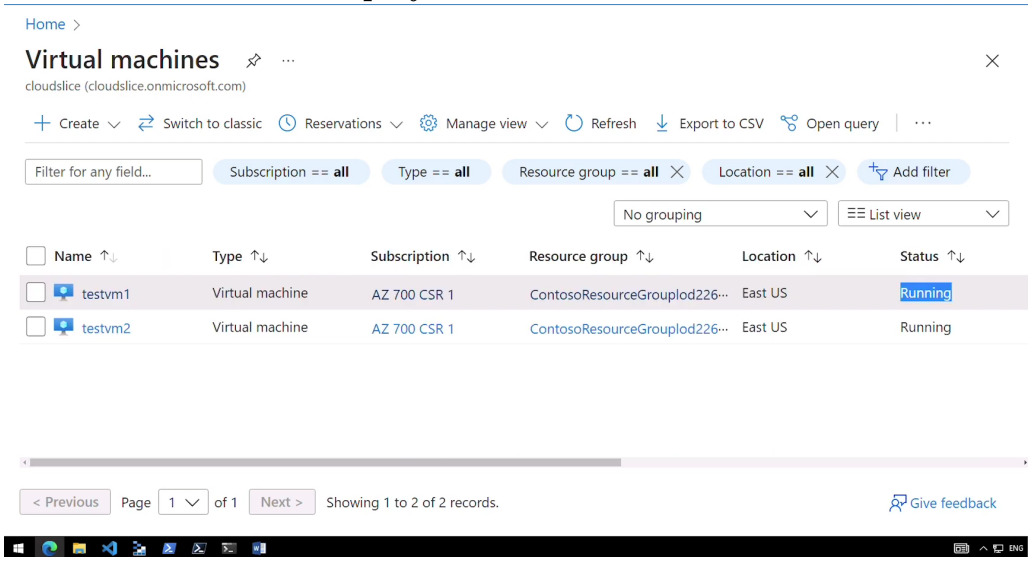
5.2.3 Step 3: Launch Virtual Machines

Create:

- Windows VM in Subnet1
- Linux VM in Subnet2

Ensure NSGs allow ICMP (ping) traffic.

Screenshot: VM Deployment

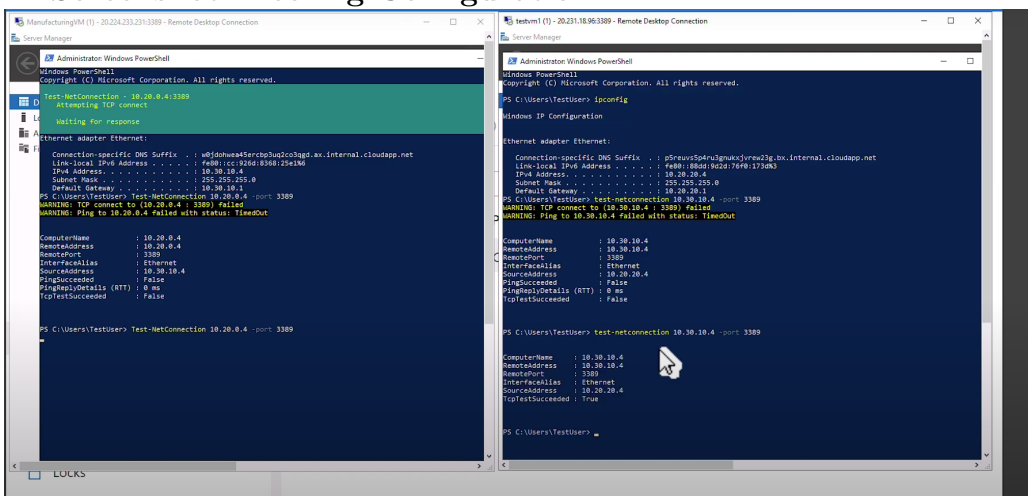


5.2.4 Step 4: Create VNet Peering

Peering must be configured from both VNets:

- Allow traffic from/to both VNets
- Check connectivity using ping from Windows to Linux VM

Screenshot: Peering Configuration



6 Conclusion

Azure VNets and Subnets enable isolated, secure network segments. VNet peering allows seamless communication between them when configured with distinct CIDRs. This setup

is essential for multi-tier applications and hybrid architectures.

References

- Microsoft Learn: https://learn.microsoft.com/en-us/azure/virtual-network/
- Azure VNet Peering Overview: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview
- CIDR Notation Explained: https://www.cloudflare.com/learning/network-layer/what-is-cidr/