

Research & Development Document: Azure Virtual Networks (VNet), Subnets, and VNet Peering

Table of Contents

1. Introduction to Azure Virtual Networks (VNet)
2. CIDR Ranges in Azure Networking
 - 2.1 VNet CIDR Range
 - 2.2 Subnet CIDR Range
 - 2.3 Best Practices for IP Addressing
3. VNet Peering
 - 3.1 What is VNet Peering?
 - 3.2 Types of VNet Peering
 - Regional (Same Region)
 - Global (Cross-Region)
 - 3.3 Peering Requirements & Limitations
4. Use Case: Implementing a VNet with Subnets and VNet Peering
 - 4.1 Prerequisites
 - 4.2 Step-by-Step Implementation
 - Create First VNet & Subnets
 - Deploy Windows & Linux VMs in Subnets
 - Create Second VNet & Establish Peering
 - Test Connectivity (Ping Between VMs)
5. Screenshots & Configuration Walkthrough
6. Troubleshooting Common Issues
7. Conclusion
8. References

1. Introduction to Azure Virtual Networks (VNet)

Azure **Virtual Network (VNet)** is a logically isolated network in Azure that provides:

- **Private IP addressing** (RFC 1918)
- **Subnet segmentation** for security & organization

- **Connectivity options** (VNet Peering, VPN, ExpressRoute)
 - **Network security groups (NSG)** for traffic control
-

2. CIDR Ranges in Azure Networking

2.1 VNet CIDR Range

- **Definition:** The primary IP address space assigned to a VNet (e.g., 10.0.0.0/16).
- **Allowed Ranges:**
 - **Class A:** 10.0.0.0/8 (16.7M IPs)
 - **Class B:** 172.16.0.0/12 (1M IPs)
 - **Class C:** 192.168.0.0/16 (65K IPs)
- **Best Practice:** Use a /16 for large deployments.

2.2 Subnet CIDR Range

- **Definition:** A segment of the VNet (e.g., 10.0.1.0/24).
- **Rules:**
 - Must be a subset of the VNet range.
 - Azure reserves **5 IPs** per subnet (First 4 + Last 1).
- **Example:**
 - Subnet: 10.0.1.0/24
 - Usable IPs: 10.0.1.4 to 10.0.1.254

2.3 Best Practices for IP Addressing

- ✓ Avoid overlapping CIDR ranges in peered VNets.
 - ✓ Reserve /24 subnets for Azure services (Gateway, Firewall).
 - ✓ Use **Network Security Groups (NSG)** to restrict traffic.
-

3. VNet Peering

3.1 What is VNet Peering?

- Connects two VNets **without a gateway**.
- Traffic flows via **Microsoft backbone** (low latency).
- **Non-transitive:** If VNetA ↔ VNetB and VNetB ↔ VNetC, VNetA ≠ VNetC.

3.2 Types of VNet Peering

Type	Description	Use Case
Regional Peering	Connects VNets in the same Azure region	Multi-tier apps
Global Peering	Connects VNets in different Azure regions	Cross-region DR

3.3 Peering Requirements & Limitations

- **No overlapping IP ranges.**
- **Max 500 peerings per VNet.**
- **Gateway transit** must be enabled for hub-spoke networks.

4. Use Case: Implementing VNet with Subnets & Peering

4.1 Prerequisites

- **Azure account** (Free Tier works).
- **Resource Group** (e.g., rg-vnet-demo).
- **Virtual Machines** (Windows & Linux).

4.2 Step-by-Step Implementation

Step 1: Create First VNet (vnet-main)

1. Go to **Azure Portal** → **Create Resource** → **Virtual Network**.
2. Configure:
 - **Name:** vnet-main
 - **Address Space:** 10.1.0.0/16
 - **Subnet 1:** subnet-win (10.1.1.0/24)
 - **Subnet 2:** subnet-linux (10.1.2.0/24)

Step 2: Deploy VMs in Subnets

1. **Windows VM** (vm-win):
 - Subnet: subnet-win
 - Private IP: 10.1.1.4
2. **Linux VM** (vm-linux):

- Subnet: subnet-linux
- Private IP: 10.1.2.4

Step 3: Create Second VNet (vnet-peer)

- **Address Space:** 10.2.0.0/16
- **Subnet:** subnet-peer (10.2.1.0/24)

Step 4: Establish VNet Peering

1. Go to vnet-main → **Peerings** → **Add Peering**.
2. Configure:
 - **Peering Link Name:** peer-main-to-peer
 - **Remote VNet:** vnet-peer
 - **Allow Forwarded Traffic:** Yes

Step 5: Test Connectivity

1. **Allow ICMP (Ping) in NSG:**
 - Add inbound rule: **ICMP** (Any source).
2. From vm-win, ping vm-linux (10.1.2.4).
3. From vm-linux, ping vm-win (10.1.1.4).

5. Screenshots & Configuration Walkthrough

(Below are key screenshots from Azure Portal)

Screenshot 1: Creating vnet-main

<https://example.com/vnet-create.png>

Screenshot 2: Adding Subnets

<https://example.com/subnet-config.png>

Screenshot 3: VNet Peering Setup

<https://example.com/peering-setup.png>

Screenshot 4: Successful Ping Test

<https://example.com/ping-test.png>

6. Troubleshooting Common Issues

✖ Ping Fails?

- Check **NSG rules** (Allow ICMP).
- Verify **VNet peering status** (Must be "Connected").

✖ IP Conflict?

- Ensure no overlapping CIDR ranges.
-

7. Conclusion

- **VNets** provide isolated network environments.
 - **Subnets** segment traffic for security.
 - **VNet Peering** enables seamless cross-VNet communication.
-

8. References

- [Azure VNet Documentation](#)
- [VNet Peering Best Practices](#)