Azure Virtual Network

Research & Development Document

CIDR Ranges, Subnets & VNet Peering

Document Information

Document Type: Research & Development (R&D)

Subject: Azure Virtual Networks, CIDR Notation, Subnets, and VNet Peering

Date: June 2025

Version: 1.0

Classification: Technical Documentation

Table of Contents

1. Executive Summary

This document provides comprehensive research and development insights into Azure Virtual Networks (VNets), focusing on CIDR range planning, subnet configuration, and Virtual Network Peering implementation. The document includes a practical use case demonstrating the creation of VNets with subnets, virtual machine deployment, and inter-VNet connectivity through peering.

> **Key Objectives:**
>
> - Understanding CIDR notation for Azure networking
> - Implementing subnet segmentation strategies
> - Configuring VNet peering for cross-network communication
> - Demonstrating practical VM connectivity scenarios

2. Introduction to Azure Virtual Networks

What is an Azure Virtual Network?

Azure Virtual Network (VNet) is a fundamental building block for private networks in Azure. It enables Azure resources to securely communicate with each other, the internet, and on-premises networks. VNets provide isolation and segmentation for workloads deployed in the Azure cloud.

Core Components of Azure VNet

> **Virtual Network Characteristics:**
>
> - **Regional Scope:** VNets are scoped to a single Azure region
> - **Subscription Boundary:** Each VNet belongs to a specific Azure subscription
> - **Address Space:** Defined using CIDR notation (IPv4 and IPv6 support)
> - **Subnets:** Logical subdivisions within the VNet address space
> - **Security:** Network Security Groups (NSGs) provide traffic filtering

Key Features:

- **Isolation:** Complete network isolation from other VNets by default
- **Connectivity:** Resources within the same VNet can communicate by default
- **Routing:** Automatic routing between subnets within a VNet
- **DNS:** Built-in name resolution services
- **Gateway Support:** VPN and ExpressRoute connectivity options

3. CIDR Notation and IP Address Planning

Understanding CIDR (Classless Inter-Domain Routing)

CIDR notation is a method for describing IP address ranges using a combination of an IP address and a prefix length. The format is `x.x.x.x/y`, where `y` represents the number of bits used for the network portion.

CIDR Examples and Calculations

CIDR Notation	Address Range	Total IPs	Usable IPs
10.0.0.0/8	10.0.0.0 - 10.255.255.255	16,777,216	16,777,214
10.0.0.0/16	10.0.0.0 - 10.0.255.255	65,536	65,534
10.0.0.0/24	10.0.0.0 - 10.0.0.255	256	254
10.0.0.0/28	10.0.0.0 - 10.0.0.15	16	14
10.0.0.0/29	10.0.0.0 - 10.0.0.7	8	6

Azure-Specific CIDR Constraints

> **VNet Address Space Requirements:**
>
> - Minimum subnet size: /29 (8 IP addresses)
> - Maximum subnet size: /2
> - IPv6 subnets must be exactly /64
> - **Azure reserves 5 IP addresses per subnet:**
>   - Network address (x.x.x.0)
>   - Default gateway (x.x.x.1)
>   - DNS mapping (x.x.x.2 and x.x.x.3)
>   - Broadcast address (x.x.x.255)

Recommended Address Spaces:

- **Small deployments:** 10.0.0.0/16 (65,536 addresses)
- **Medium deployments:** 10.0.0.0/12 (1,048,576 addresses)
- **Large deployments:** 10.0.0.0/8 (16,777,216 addresses)

4. Azure Virtual Network Subnets

Subnet Design Principles

Subnets provide logical segmentation within a VNet, enabling better security, management, and traffic control. Each subnet represents a range of IP addresses within the VNet's address space.

> **Subnet Planning Considerations:**
>
> - **Application Tiers:** Separate web, application, and database layers
> - **Security Zones:** DMZ, internal, and secure zones
> - **Service Requirements:** Different Azure services may require dedicated subnets
> - **Future Growth:** Plan for scalability and expansion

Subnet Types and Use Cases

Subnet Type	CIDR Example	Use Cases
Web Tier Subnet	10.0.1.0/24	Public-facing web servers, Load balancers, Application gateways
Application Tier Subnet	10.0.2.0/24	Application servers, Business logic components, API services
Database Tier Subnet	10.0.3.0/24	Database servers, Storage services, Backup systems
Management Subnet	10.0.10.0/24	Jump boxes, Monitoring systems, Administrative tools

Network Security Groups (NSGs)

NSGs act as virtual firewalls, controlling traffic flow to and from subnets and network interfaces.

> **NSG Rule Components:**
>
> - **Priority:** Lower numbers have higher priority (100-4096)
> - **Source/Destination:** IP addresses, service tags, or application security groups
> - **Protocol:** TCP, UDP, or Any
> - **Port Ranges:** Specific ports or ranges
> - **Action:** Allow or Deny

5. Virtual Network Peering

VNet Peering Overview

Virtual Network Peering enables seamless connectivity between Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes, with traffic routed through Microsoft's backbone infrastructure.

Types of VNet Peering

1. Regional VNet Peering

- Connects VNets within the same Azure region
- Low latency, high bandwidth connectivity
- No bandwidth limitations beyond VM limits
- Private IP address communication only

2. Global VNet Peering

- Connects VNets across different Azure regions
- Global connectivity through Microsoft backbone
- Slightly higher latency compared to regional peering
- Cross-region data transfer charges apply

VNet Peering Benefits

Performance Advantages:

- High bandwidth, low latency connections
- Traffic remains on Microsoft backbone network
- No encryption overhead (traffic is inherently secure)
- No single point of failure or bandwidth bottleneck

Operational Benefits:

- Simple configuration and management
- Automatic route propagation
- No gateway requirements
- Cross-subscription peering support

Peering Configuration Options

Setting	Description
Allow virtual network access	Enables communication between peered VNets
Allow forwarded traffic	Permits traffic forwarded by network virtual appliances
Allow gateway transit	Allows remote VNet to use local VNet's VPN gateway
Use remote gateways	Uses the remote VNet's VPN gateway

6. Prerequisites for Implementation

Azure Subscription Requirements

Account Setup:

- Valid Azure subscription with sufficient credits
- Appropriate permissions (Contributor or Owner role)
- Resource Group creation permissions
- Virtual Machine creation quota

Regional Considerations:

- Select regions that support all required services
- Consider latency requirements for multi-region deployments
- Verify service availability in chosen regions

Resource Planning

Resource Type	Requirements
Compute Resources	VM sizes, OS licensing, Storage accounts, Network interfaces
Network Resources	IP address space, Subnet segmentation, NSG rules, DNS configuration
Management Tools	Azure Portal access, CLI/PowerShell, ARM templates, IaC tools

7. Use Case Implementation

Scenario Description

Implementation Objectives:

1. **VNet Creation:** Deploy two virtual networks with proper CIDR planning
2. **Subnet Configuration:** Create multiple subnets within each VNet
3. **VM Deployment:** Launch Windows and Linux VMs in different subnets
4. **Connectivity Testing:** Verify inter-subnet communication within VNet
5. **VNet Peering:** Establish connectivity between the two VNets
6. **Cross-VNet Communication:** Test VM connectivity across peered VNets

Architecture Overview

Component	Production VNet	Development VNet
Address Space	10.1.0.0/16	10.2.0.0/16
Subnet 1	Web: 10.1.1.0/24 (Windows VM)	Dev: 10.2.1.0/24 (Windows VM)
Subnet 2	App: 10.1.2.0/24 (Linux VM)	Test: 10.2.2.0/24 (Linux VM)
Location	East US	West US 2

Architecture Diagram Placeholder
Insert network topology diagram showing both VNets, subnets, VMs, and peering connection

8. Step-by-Step Configuration Guide

Phase 1: Create First Virtual Network (Production VNet)

Step 1: Navigate to Virtual Networks

1. Log into Azure Portal (portal.azure.com)
2. Click "Create a resource" → "Networking" → "Virtual network"
3. Alternatively, search for "Virtual networks" in the search bar

Step 2: Configure Basic Settings

```
Resource Group: rg-networking-demo
Virtual Network Name: vnet-production-eastus
Region: East US
```

Screenshot Placeholder
Insert Azure Portal screenshot of VNet basic configuration page

Step 3: Configure IP Addresses

```
IPv4 Address Space: 10.1.0.0/16

Subnets:
- Name: subnet-web
  Address Range: 10.1.1.0/24

- Name: subnet-app
  Address Range: 10.1.2.0/24
```

Screenshot Placeholder
Insert Azure Portal screenshot of IP address configuration

Phase 2: Create Second Virtual Network (Development VNet)

```
Resource Group: rg-networking-demo
Virtual Network Name: vnet-development-westus2
Region: West US 2
IPv4 Address Space: 10.2.0.0/16

Subnets:
- Name: subnet-dev
  Address Range: 10.2.1.0/24

- Name: subnet-test
  Address Range: 10.2.2.0/24
```

Phase 3: Deploy Virtual Machines

Windows VM Configuration (Production VNet)

Setting	Value
Resource Group	rg-networking-demo
VM Name	vm-win-prod-web
Region	East US
Image	Windows Server 2022 Datacenter
Size	Standard_B2s (2 vcpus, 4 GiB memory)
Virtual Network	vnet-production-eastus
Subnet	subnet-web (10.1.1.0/24)

Screenshot Placeholder
Insert Azure Portal screenshot of VM creation - Basic settings

Screenshot Placeholder
Insert Azure Portal screenshot of VM creation - Networking settings

Phase 4: Test Intra-VNet Connectivity

Connectivity Testing Steps:

1. Connect to Windows VM via RDP
2. Test ping to Linux VM in same VNet
3. Verify port connectivity using telnet
4. Document IP addresses and results

PowerShell Commands for Testing:

```
# From Windows VM command prompt
ping 10.1.2.4  # Private IP of Linux VM in app subnet
Test-NetConnection 10.1.2.4 -Port 22
```

Linux Commands for Testing:

```
# SSH to Linux VM
ssh azureuser@<public-ip-address>

# Test connectivity to Windows VM
ping 10.1.1.4  # Private IP of Windows VM in web subnet
telnet 10.1.1.4 3389
```

Screenshot Placeholder
Insert screenshot of successful ping test between VMs in same VNet

Phase 5: Configure VNet Peering

Critical Peering Requirements:

- Ensure no overlapping CIDR ranges between VNets
- Verify proper permissions on both VNets
- Configure bidirectional peering for full connectivity

Step 1: Create Peering from Production to Development VNet

1. Navigate to vnet-production-eastus in Azure Portal
2. Select "Peerings" under Settings
3. Click "+ Add" to create new peering

Peering Setting	Value
Peering Link Name	prod-to-dev-peering

Peering Setting	Value
Remote Virtual Network	vnet-development-westus2
Allow virtual network access (local to remote)	Enabled
Allow virtual network access (remote to local)	Enabled
Allow forwarded traffic	Disabled
Allow gateway transit	Disabled

Screenshot Placeholder
Insert Azure Portal screenshot of VNet peering configuration

Step 2: Verify Peering Status

- Check peering status shows "Connected"
- Verify both directions are properly configured
- Review effective routes in VM network interfaces

Screenshot Placeholder
Insert screenshot showing successful peering status as "Connected"

Phase 6: Test Cross-VNet Connectivity

Testing from Production to Development VNet

```
# From Windows VM in Production VNet
ping 10.2.1.4  # Windows VM in Development VNet
ping 10.2.2.4  # Linux VM in Development VNet
Test-NetConnection 10.2.1.4 -Port 3389
Test-NetConnection 10.2.2.4 -Port 22
```

Testing from Development to Production VNet

```
# From Linux VM in Development VNet
ping 10.1.1.4  # Windows VM in Production VNet
ping 10.1.2.4  # Linux VM in Production VNet
telnet 10.1.1.4 3389
```

Verify Network Routes

```
# Windows: Check routing table
route print

# Linux: Check routing table
ip route show
netstat -rn
```

Screenshot Placeholder
Insert screenshot of successful cross-VNet ping test results

Phase 7: Configure Network Security Groups

Create Custom NSG Rules

Rule Name	Priority	Protocol	Ports	Action
Allow-ICMP-Inbound	1000	ICMP	*	Allow
Allow-RDP-Inbound	1010	TCP	3389	Allow
Allow-SSH-Inbound	1020	TCP	22	Allow

Screenshot Placeholder
Insert Azure Portal screenshot of NSG rule configuration

9. Best Practices and Recommendations

Network Design Best Practices

IP Address Planning:

- Use private IP ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
- Avoid overlapping address spaces between VNets
- Plan for future growth and expansion
- Document IP allocation and usage

Subnet Segmentation Strategy

- Separate application tiers into different subnets
- Use dedicated subnets for specific Azure services
- Implement network security groups at subnet level
- Consider subnet size based on expected resource count

Security Considerations

- Implement least-privilege access principles
- Use Network Security Groups for traffic filtering
- Consider Azure Firewall for advanced protection
- Enable Azure DDoS Protection for internet-facing resources

Performance Optimization

Optimization Area	Recommendations
VNet Peering	Use regional peering when possible, Monitor bandwidth usage, Optimize traffic patterns
VM Placement	Deploy in same availability zone, Use proximity placement groups, Enable accelerated networking
Network Monitoring	Enable Network Watcher, Configure flow logs, Set up performance alerts

Cost Management

Cost Optimization Strategies:

- **Regional vs Global Peering:** Global peering incurs data transfer charges
- **VM Right-sizing:** Choose appropriate VM sizes for workloads
- **Reserved Instances:** Use for predictable, long-term workloads
- **Auto-shutdown:** Implement for development environments

10. Troubleshooting Common Issues

Connectivity Issues

Problem: VMs Cannot Communicate Within Same VNet

> **Diagnostic Steps:**
>
> 1. Verify VM network configuration and IP assignments
> 2. Check NSG rules on subnet and NIC level
> 3. Validate effective security rules in Azure Portal
> 4. Test with simplified NSG rules (allow all)
> 5. Check Windows Firewall and Linux iptables settings

Common Solutions:

- Ensure NSGs allow required protocols and ports
- Verify VMs are deployed in correct subnets
- Check operating system firewall configurations
- Validate VM network interface settings

Problem: Cross-VNet Communication Fails After Peering

> **Diagnostic Checklist:**
>
> - ✓ Verify peering status shows "Connected" in both directions
> - ✓ Check for CIDR address space overlaps
> - ✓ Validate effective routes on VM network interfaces
> - ✓ Test connectivity with traceroute/tracert
> - ✓ Review NSG rules for cross-VNet traffic

Performance Issues

Issue	Possible Causes	Solutions
High Latency	Global peering, VM location, Network congestion	Use regional peering, Enable accelerated networking, Optimize placement
Low Bandwidth	VM size limitations, Network throttling	Upgrade VM size, Check bandwidth limits, Monitor utilization

Issue	Possible Causes	Solutions
Connection Drops	NSG rules, VM issues, Network instability	Review logs, Update configurations, Implement retry logic

Security and Access Issues

Problem: Cannot Access VMs via Public IP

```
# Diagnostic Commands
nslookup <public-ip>
telnet <public-ip> <port>
curl -v <public-ip>:<port>
```

Resolution Steps:

1. Verify public IP is properly allocated and associated
2. Check NSG rules allow traffic from your source IP
3. Validate RDP/SSH services are running on VMs
4. Review Azure Security Center recommendations
5. Consider using Azure Bastion for secure access

11. Conclusion

Project Summary

This comprehensive R&D document has successfully demonstrated the implementation of Azure Virtual Networks with advanced networking features. The practical use case showcased the complete lifecycle of VNet deployment, from initial planning through operational testing.

> **Key Achievements:**
>
> - **Technical Implementation:** Successfully deployed two VNets with proper CIDR planning across different Azure regions
> - **Subnet Configuration:** Implemented logical network segmentation with appropriate address allocation
> - **VM Deployment:** Deployed Windows and Linux virtual machines across multiple subnets
> - **Connectivity Validation:** Verified both intra-VNet and cross-VNet communication capabilities
> - **Peering Implementation:** Established global VNet peering between East US and West US 2 regions

Technical Learnings

CIDR Planning Insights:

- Proper address space allocation prevents future connectivity issues
- Azure's reservation of 5 IP addresses per subnet must be factored into planning
- Non-overlapping address spaces are critical for successful VNet peering

VNet Peering Benefits Realized:

- Seamless cross-region connectivity without VPN overhead
- Low-latency communication through Microsoft backbone network
- Simplified network architecture compared to gateway-based solutions

Future Enhancement Opportunities

> **Scalability Improvements:**
>
> - **Hub-and-Spoke Topology:** Implement centralized connectivity model for larger deployments
> - **Azure Virtual WAN:** Consider for global, software-defined network architecture
> - **ExpressRoute Integration:** Add hybrid connectivity for on-premises resources
> - **Network Automation:** Implement Infrastructure as Code using ARM templates or Terraform

Security Enhancements:

- Deploy Azure Firewall for centralized network security management
- Implement Azure Private Link for secure service connectivity
- Configure Just-In-Time VM access for enhanced security
- Enable Azure Sentinel for security monitoring and threat detection

Operational Excellence:

- Implement comprehensive network monitoring with Azure Network Watcher
- Configure automated alerting for network performance and security events
- Establish network performance baselines and SLA metrics
- Create detailed runbooks for common network operations and troubleshooting

Business Value Delivered

Value Category	Benefits Achieved
Cost Optimization	Eliminated need for complex VPN gateways, Reduced operational overhead
Performance	Low-latency cross-region connectivity, High-bandwidth inter-VNet communication
Security	Private IP communication, Network isolation, Centralized security policies
Scalability	Easy expansion capabilities, Support for multiple regions, Flexible addressing

Recommendations for Production Deployment

> ### Critical Production Considerations:
>
> 1. **High Availability:** Deploy VMs across multiple availability zones
> 2. **Backup and Recovery:** Implement comprehensive backup strategies
> 3. **Monitoring:** Deploy full-stack monitoring solutions
> 4. **Security:** Implement defense-in-depth security strategies
> 5. **Compliance:** Ensure adherence to regulatory requirements
> 6. **Documentation:** Maintain current network documentation and procedures

Final Thoughts

Azure Virtual Networks provide a robust foundation for cloud infrastructure, offering enterprise-grade networking capabilities with simplified management. The combination of proper CIDR planning, strategic subnet design, and VNet peering creates a scalable and secure network architecture suitable for diverse workload requirements.

This implementation demonstrates that Azure's networking services can effectively support complex, multi-region deployments while maintaining performance, security, and cost efficiency. The knowledge gained through this practical exercise provides a solid foundation for implementing production-grade Azure networking solutions.

Document Classification: Technical Documentation | **Version:** 1.0 | **Date:** June 2025

Author: Azure Networking Team | **Review:** Technical Architecture Review Board

Next Review Date: December 2025 | **Distribution:** Technical Teams, Management