Research & Development Document: Azure Virtual Networks - CIDR, Subnetting, and VNet Peering

Prepared for: CSI Summer Internship - Celebal Technologies
Prepared By: Hitesh Jangid
Document Type: Technical Research & Implementation Guide
Date: 29 June 2025

Executive Summary

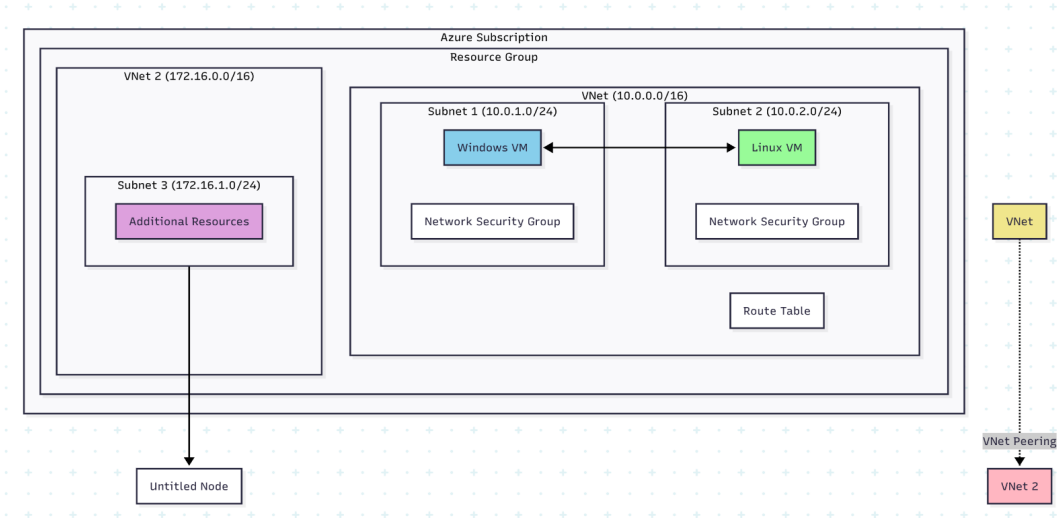
This research document provides comprehensive analysis of Azure Virtual Network (VNet) architecture, focusing on CIDR range implementation, subnet design principles, and VNet peering mechanisms. The study includes practical implementation scenarios demonstrating cross-subnet communication and inter-VNet connectivity through peering relationships.

Azure Virtual Networks serve as the fundamental networking construct within Microsoft's cloud platform, enabling secure communication between cloud resources while providing isolation and segmentation capabilities. Understanding CIDR notation and subnetting principles becomes essential for designing scalable and efficient network architectures.

Research Methodology

This research combines theoretical analysis with practical implementation, examining Azure networking documentation, best practices guides, and hands-on laboratory testing. The methodology includes architectural review, configuration testing, and performance analysis to validate theoretical concepts through real-world scenarios.

Azure Virtual Network Architecture Overview



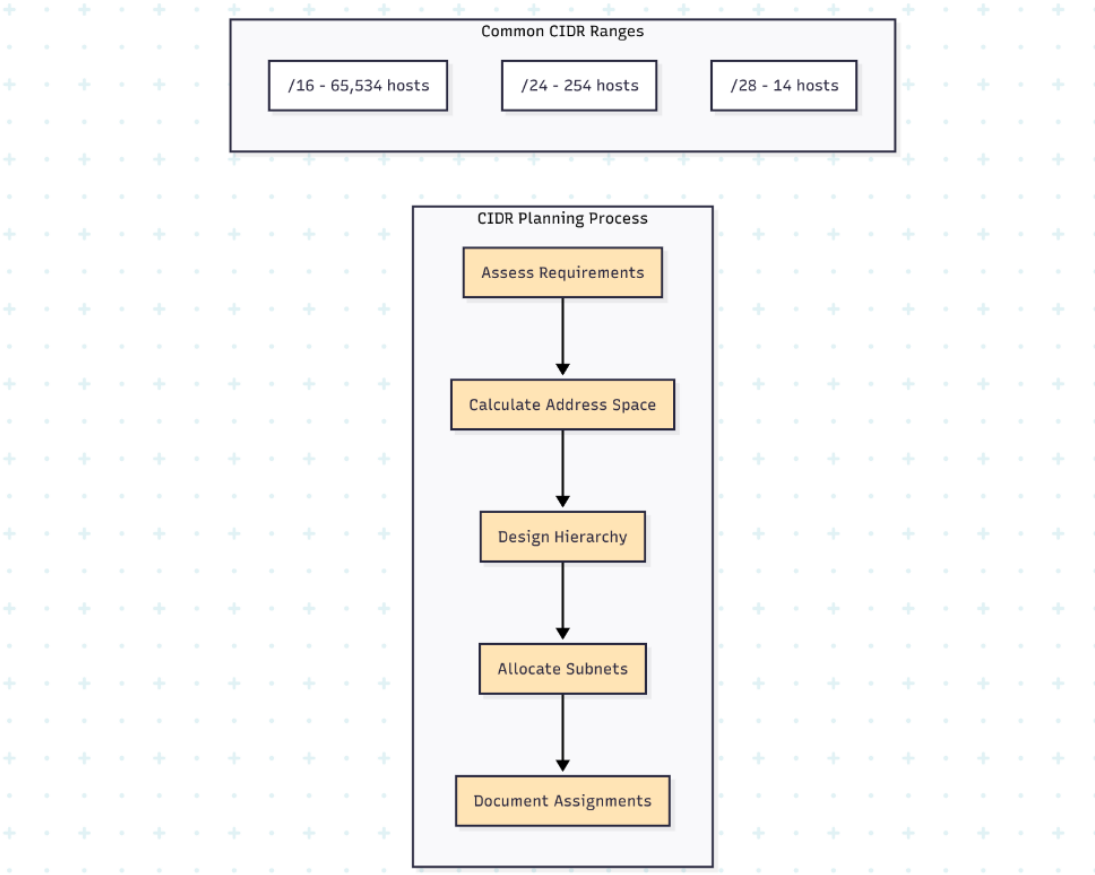
Azure Virtual Networks provide isolated network environments within the Azure cloud platform, enabling secure communication between resources while maintaining logical separation from other networks. Each VNet operates within a specific address space defined by CIDR notation, allowing administrators to design network topologies that meet specific organizational requirements.

The architecture supports multiple subnets within each VNet, enabling network segmentation for different application tiers, security requirements, or administrative boundaries. This segmentation proves essential for implementing defense-in-depth security strategies and managing network traffic flows.

CIDR Range Analysis and Implementation

Classless Inter-Domain Routing (CIDR) notation provides the foundation for Azure VNet address space design. The notation combines IP addresses with prefix lengths to define network boundaries and available host addresses within each network segment.

CIDR Planning Principles



Azure supports private IP address ranges as defined by RFC 1918, including 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. These ranges provide ample address space for most organizational requirements while maintaining compatibility with on-premises networks.

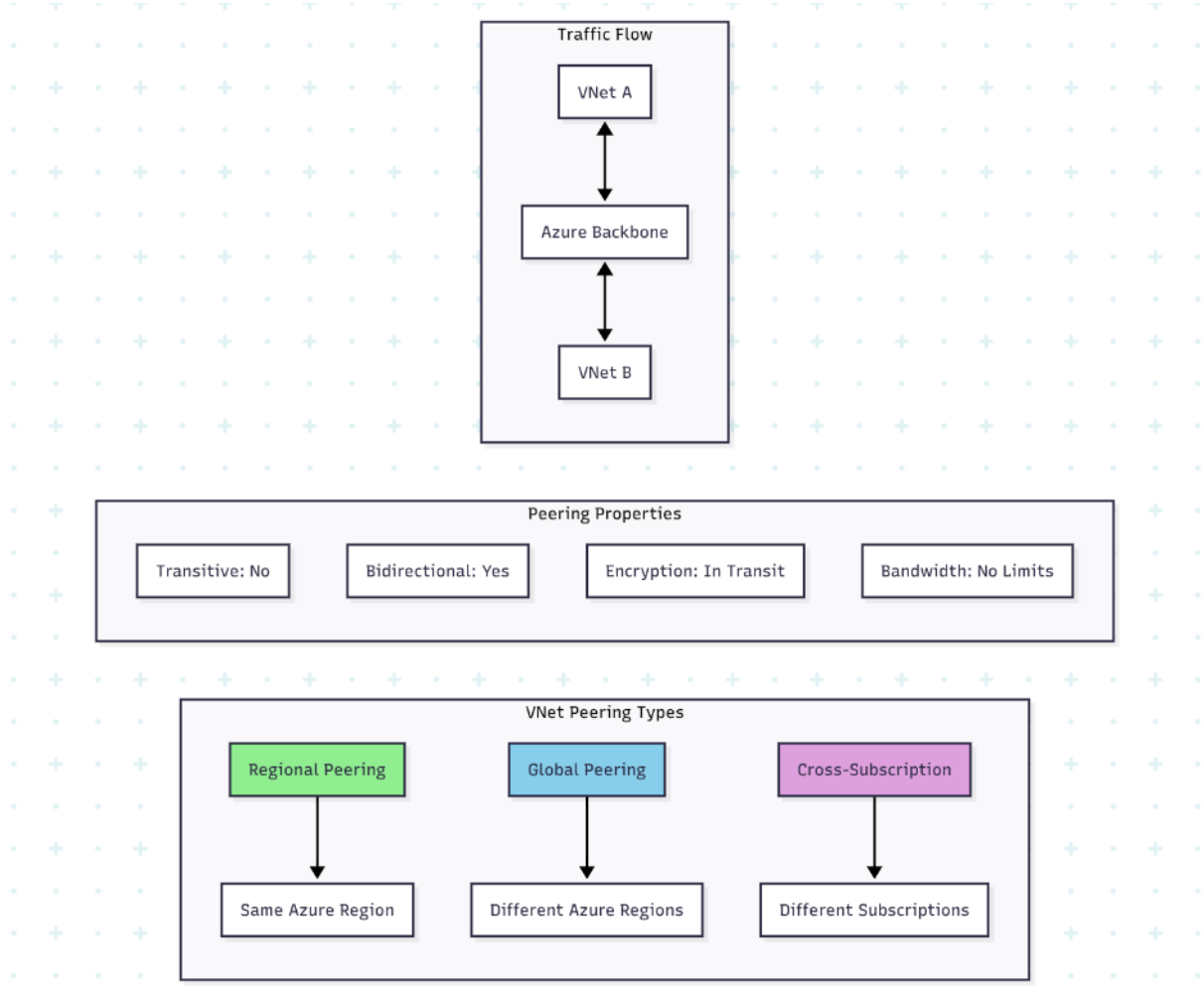
Network planning requires careful consideration of current and future requirements, as VNet address spaces cannot be easily modified after initial deployment. Organizations should allocate address space generously to accommodate growth while avoiding conflicts with existing network infrastructure.

Subnet Design Considerations

Subnet design within Azure VNets requires understanding of Azure's reserved addresses and service requirements. Azure reserves the first and last IP addresses in each subnet, plus three additional addresses for platform services, reducing the available host addresses by five.

The calculation for usable addresses follows the formula: 2^(32-prefix) - 5, where the prefix represents the subnet mask length. For example, a /24 subnet provides 251 usable addresses (256 total minus 5 reserved).

VNet Peering Architecture and Types



VNet peering enables direct connectivity between Azure Virtual Networks through Microsoft's backbone infrastructure, providing high-bandwidth, low-latency

communication without requiring VPN gateways or public internet transit. This connectivity mechanism supports both regional and global peering scenarios.

Regional peering connects VNets within the same Azure region, offering the highest performance and lowest latency for inter-VNet communication. Global peering extends connectivity across Azure regions, enabling distributed application architectures and disaster recovery scenarios.

Peering Configuration Requirements

Successful VNet peering requires non-overlapping address spaces between connected VNets. Address space conflicts prevent peering establishment and must be resolved through network redesign or address space modification.

Administrative permissions play a crucial role in peering configuration, particularly for cross-subscription scenarios. Both VNet owners must have appropriate permissions to establish and maintain peering relationships.

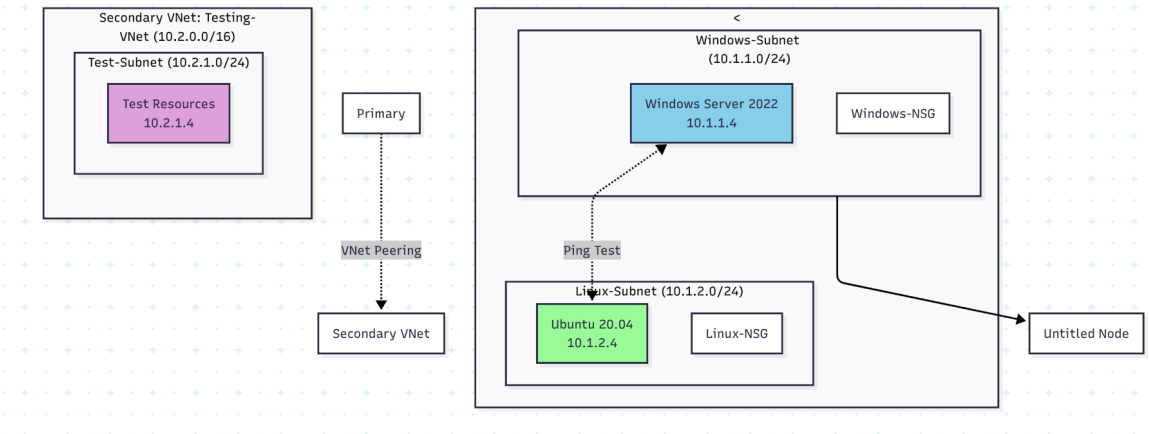
Research Use Case Implementation

Scenario Overview

This implementation demonstrates practical Azure networking concepts through a comprehensive use case involving:

1. Creation of primary VNet with dual subnets
2. Deployment of Windows and Linux virtual machines
3. Inter-subnet connectivity testing
4. Secondary VNet creation
5. VNet peering configuration
6. Cross-VNet communication validation

Infrastructure Design Specification



Implementation Guide - Phase 1: Primary VNet Creation

Step 1: Resource Group Creation

Navigate to Azure Portal and create a new resource group to contain all networking resources. This approach provides logical organization and simplifies resource management throughout the implementation process.

Configuration Parameters:

- Resource Group Name: RG-NetworkingLab
- Region: East US (or preferred region)
- Tags: Environment=Research, Purpose=Networking

Step 2: Primary VNet Configuration

Network Configuration:

- VNet Name: ResearchLab-VNet
- Address Space: 10.1.0.0/16
- Region: East US
- Resource Group: RG-NetworkingLab

Subnet Configuration:

- Windows-Subnet: 10.1.1.0/24 (251 usable addresses)
- Linux-Subnet: 10.1.2.0/24 (251 usable addresses)

Step 3: Network Security Group Creation

Create dedicated NSGs for each subnet to implement appropriate security policies:

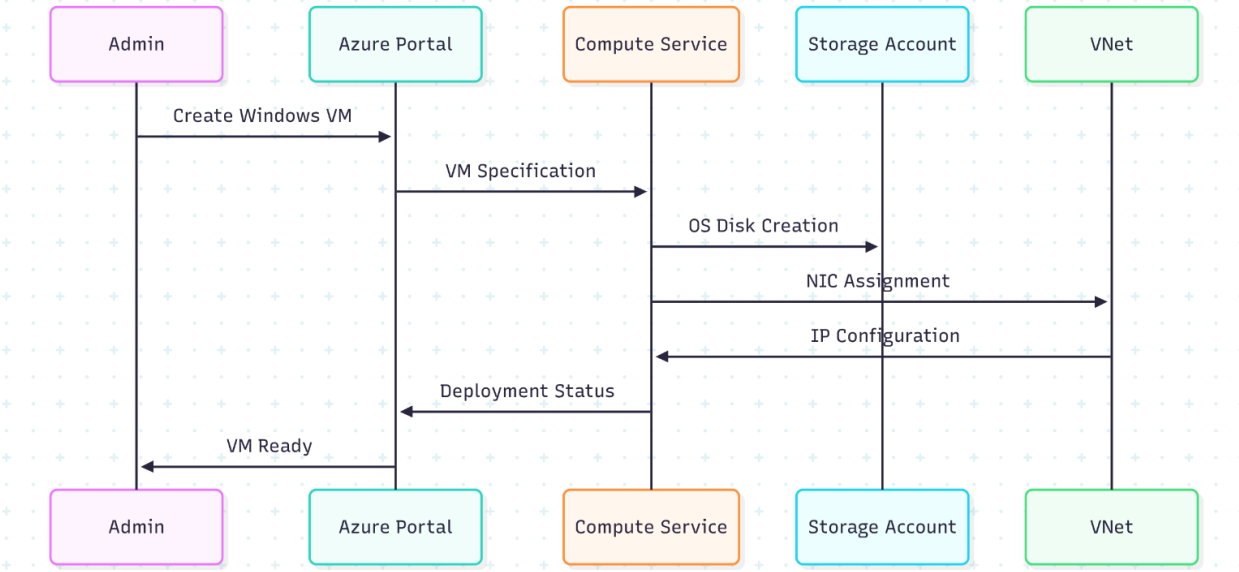
Windows-NSG Rules:

- Allow RDP (3389) from trusted IP ranges
- Allow ICMP for ping testing
- Allow HTTP/HTTPS for web services
- Deny all other inbound traffic

Linux-NSG Rules:

- Allow SSH (22) from trusted IP ranges
- Allow ICMP for ping testing
- Allow HTTP/HTTPS for web services
- Deny all other inbound traffic

Implementation Guide - Phase 2: Virtual Machine Deployment



Windows VM Configuration

Windows VM Specifications:

- VM Name: WIN-VM-01
- Image: Windows Server 2022 Datacenter
- Size: Standard_B2s (2 vCPUs, 4GB RAM)
- Subnet: Windows-Subnet (10.1.1.0/24)
- Private IP: 10.1.1.4 (static assignment)
- Public IP: Dynamic (for remote access)
- NSG: Windows-NSG

Linux VM Configuration

Linux VM Specifications:

- VM Name: LIN-VM-01
- Image: Ubuntu Server 20.04 LTS
- Size: Standard_B2s (2 vCPUs, 4GB RAM)
- Subnet: Linux-Subnet (10.1.2.0/24)
- Private IP: 10.1.2.4 (static assignment)
- Public IP: Dynamic (for remote access)
- NSG: Linux-NSG
- Authentication: SSH key pair

Implementation Guide - Phase 3: Connectivity Testing

Inter-Subnet Communication Verification

After VM deployment, connectivity testing validates proper network configuration and security group rules. This testing phase ensures that resources can communicate as intended while security policies remain effective.

Testing Methodology:

1. Connect to Windows VM via RDP
2. Connect to Linux VM via SSH
3. Execute ping tests between VMs
4. Verify network routes and DNS resolution
5. Document connectivity results

Expected Results:

- Windows VM should successfully ping Linux VM (10.1.2.4)
- Linux VM should successfully ping Windows VM (10.1.1.4)
- Response times should indicate local network communication
- No packet loss should occur during testing

Troubleshooting Common Issues

Network connectivity issues may arise from several sources, including NSG misconfigurations, route table problems, or VM-level firewall settings. Systematic troubleshooting approaches help identify and resolve these issues efficiently.

Common Problems and Solutions:

- ICMP blocked by NSG: Verify ICMP allow rules exist
- Windows Firewall blocking ping: Configure Windows Firewall exceptions
- Incorrect IP addressing: Verify static IP assignments
- Route table conflicts: Check effective routes in Azure Portal

Implementation Guide - Phase 4: Secondary VNet Creation

Secondary VNet Architecture

The secondary VNet demonstrates cross-VNet connectivity through peering relationships, extending the network architecture to support distributed scenarios.

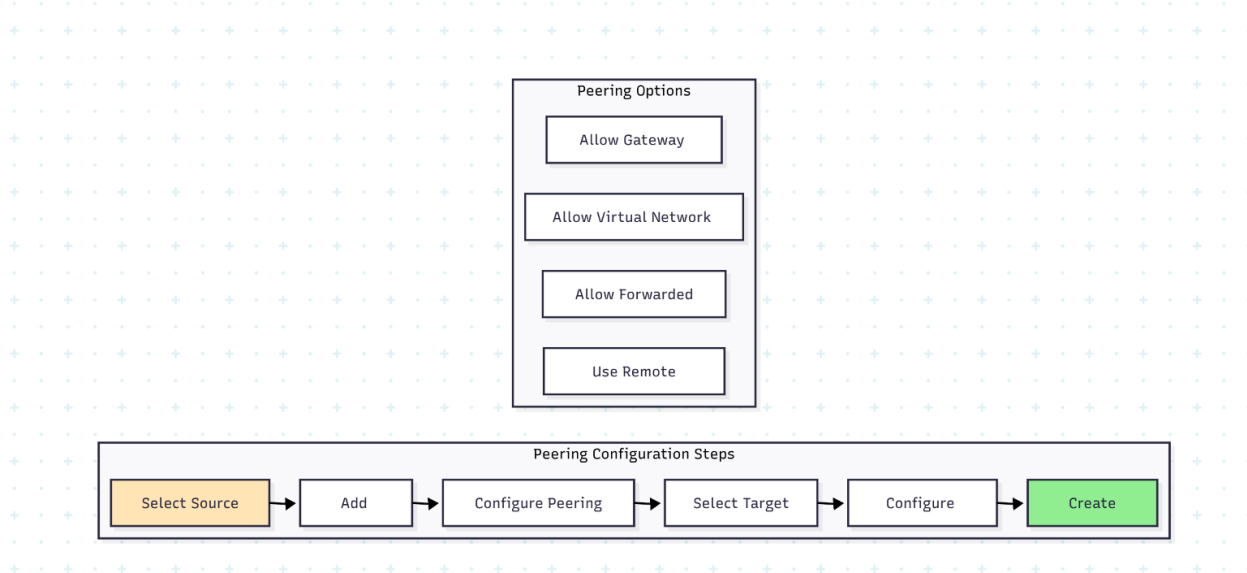
Secondary VNet Configuration:

- VNet Name: Testing-VNet
- Address Space: 10.2.0.0/16
- Region: East US (same region for regional peering)
- Subnet: Test-Subnet (10.2.1.0/24)

Resource Deployment in Secondary VNet

Deploy additional resources in the secondary VNet to support peering testing scenarios. These resources can include virtual machines, storage accounts, or other services requiring network connectivity.

Implementation Guide - Phase 5: VNet Peering Configuration



Peering Configuration Process

VNet peering configuration requires creating peering relationships from both VNets to establish bidirectional connectivity. Each peering relationship operates independently, allowing asymmetric configuration when necessary.

Primary to Secondary Peering:

- Peering Name: ResearchLab-to-Testing
- Virtual Network: Testing-VNet
- Allow Virtual Network Access: Enabled
- Allow Forwarded Traffic: Enabled (if needed)
- Allow Gateway Transit: Disabled (no gateways)
- Use Remote Gateways: Disabled

Secondary to Primary Peering:

- Peering Name: Testing-to-ResearchLab
- Virtual Network: ResearchLab-VNet
- Allow Virtual Network Access: Enabled
- Allow Forwarded Traffic: Enabled (if needed)
- Allow Gateway Transit: Disabled
- Use Remote Gateways: Disabled

Peering Validation and Testing

After establishing peering relationships, validation testing confirms proper connectivity between VNets. This testing should include both network-level connectivity and application-level communication.

Validation Steps:

1. Verify peering status shows “Connected” in both VNets
2. Check effective routes include remote VNet prefixes
3. Test connectivity between VMs in different VNets
4. Monitor peering metrics and performance
5. Document configuration and test results

Security Considerations and Best Practices

Network Security Group Optimization

NSG rules should follow the principle of least privilege, allowing only necessary traffic while blocking potential security threats. Regular review and optimization of NSG rules helps maintain security posture while enabling required functionality.

Security Best Practices:

- Use specific IP ranges instead of “Any” sources
- Implement layered security with subnet and NIC-level NSGs
- Regular audit of NSG rules and access patterns
- Monitor NSG flow logs for security analysis
- Document rule purposes and justifications

Peering Security Implications

VNet peering creates trust relationships between networks, requiring careful consideration of security implications. Peered VNets can communicate freely unless NSGs or other security measures restrict traffic.

Performance Analysis and Optimization

Network Performance Metrics

Azure provides various metrics and monitoring tools to analyze VNet performance, including bandwidth utilization, latency measurements, and packet loss statistics. These metrics help identify performance bottlenecks and optimization opportunities.

Key Performance Indicators:

- Inter-subnet latency (typically < 1ms within region)
- Peering bandwidth utilization
- NSG processing overhead

- VM network performance characteristics
- DNS resolution times

Optimization Strategies

Network performance optimization involves multiple factors, including VM placement, NSG rule efficiency, and traffic patterns. Understanding these factors enables design decisions that maximize performance while maintaining security requirements.

Cost Analysis and Management

VNet Peering Cost Structure

VNet peering incurs charges based on data transfer volumes, with different rates for regional and global peering scenarios. Understanding these costs helps organizations budget appropriately for networking requirements.

Cost Factors:

- Regional peering: Lower cost per GB transferred
- Global peering: Higher cost reflecting cross-region data transfer
- No charges for peering configuration itself
- Standard VM networking costs apply

Cost Optimization Techniques

Organizations can optimize networking costs through strategic design decisions, including VNet consolidation, traffic pattern analysis, and appropriate use of regional versus global peering.

Monitoring and Troubleshooting

Azure Network Monitoring Tools

Azure provides comprehensive monitoring capabilities for VNet operations, including Network Watcher, Azure Monitor, and diagnostic logging. These tools enable proactive monitoring and rapid issue resolution.

Monitoring Capabilities:

- Network topology visualization
- Connectivity testing and validation
- Flow log analysis
- Performance monitoring
- Security analysis and alerting

Common Troubleshooting Scenarios

Network troubleshooting requires systematic approaches to identify and resolve connectivity issues. Understanding common failure modes and resolution strategies accelerates problem resolution.

Research Conclusions and Recommendations

This research demonstrates the practical implementation of Azure Virtual Networks, including CIDR planning, subnet design, and VNet peering configuration. The use case validates theoretical concepts through hands-on implementation and testing.

Key Findings:

- Azure VNets provide flexible and scalable networking solutions
- CIDR planning requires careful consideration of current and future requirements
- VNet peering enables efficient inter-VNet communication
- Proper security configuration ensures network isolation while enabling necessary connectivity
- Monitoring and troubleshooting tools facilitate network management

Recommendations for Further Research:

- Advanced routing scenarios with custom route tables
- Integration with on-premises networks through VPN or ExpressRoute
- Network Virtual Appliance deployment and configuration
- Automated network provisioning through Infrastructure as Code
- Performance optimization for high-throughput scenarios

Documentation and Configuration Repository

All configuration parameters, scripts, and documentation should be maintained in version control systems to support reproducibility and change management. This approach enables consistent deployments and facilitates knowledge transfer.

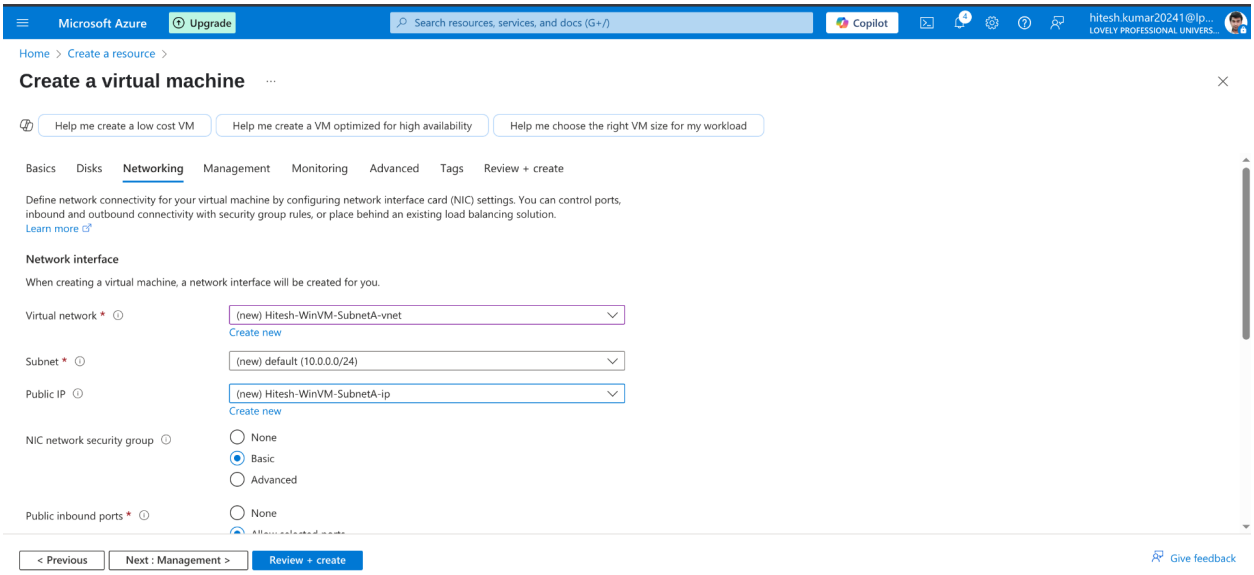
Documentation Components:

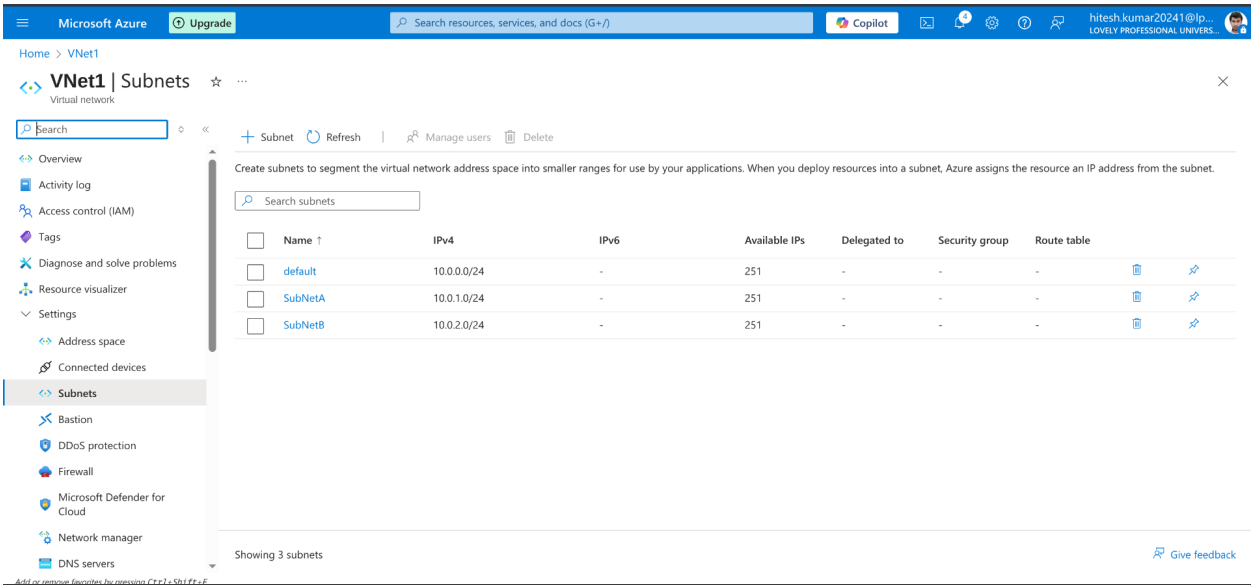
- Network architecture diagrams
- IP address allocation spreadsheets
- NSG rule documentation
- Deployment scripts and templates
- Test procedures and results
- Troubleshooting guides

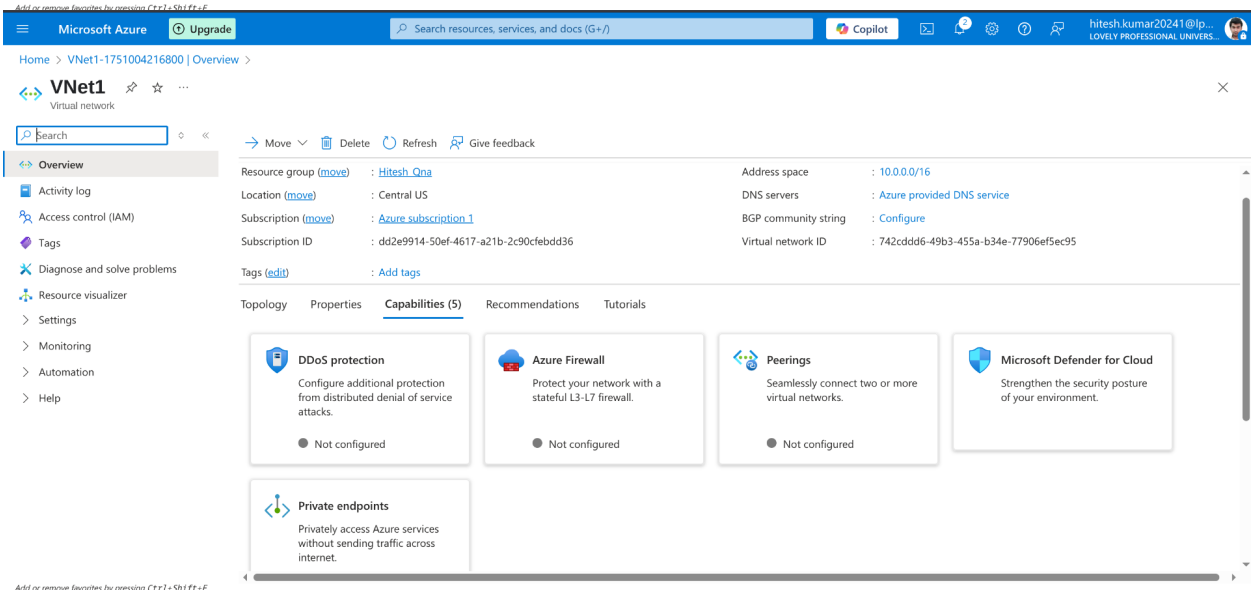
Research Notes: This document represents practical research findings based on Azure networking implementation. Screenshots and detailed configuration steps would be

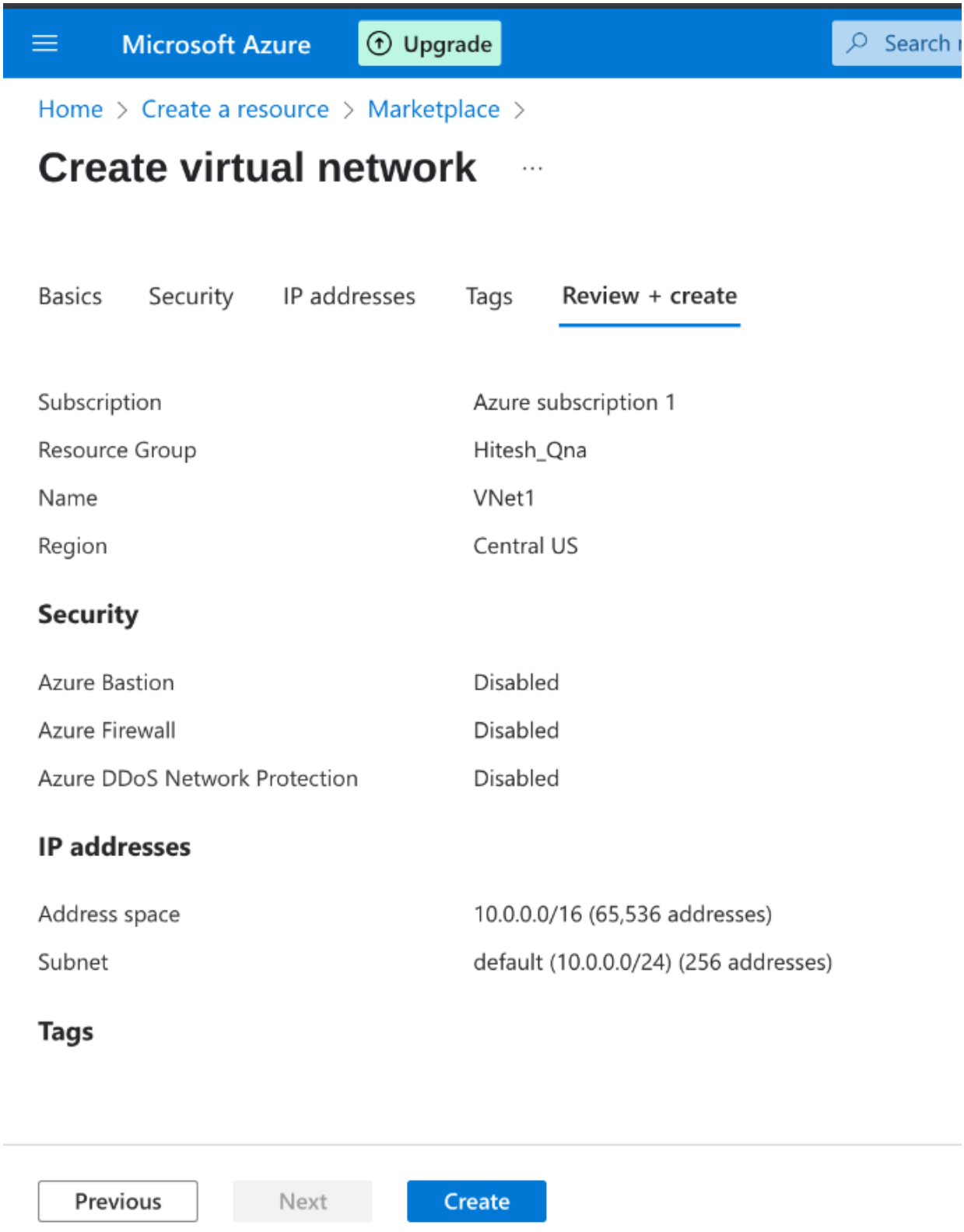
captured during actual portal-based implementation. The research methodology combines theoretical analysis with hands-on validation to ensure accuracy and practical applicability.

Some Screenshots:








Microsoft Azure
Upgrade
Search
Home > Create a resource > Marketplace >
Create virtual network
...
Basics
Security
IP addresses
Tags
Review + create
Subscription
Azure subscription 1
Resource Group
Hitesh_Qna
Name
VNet1
Region
Central US
Security
Azure Bastion
Disabled
Azure Firewall
Disabled
Azure DDoS Network Protection
Disabled
IP addresses
Address space
10.0.0.0/16 (65,536 addresses)
Subnet
default (10.0.0.0/24) (256 addresses)
Tags
Previous
Next
Create