CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Harsh Tongariya

College: Arya College of Engineering Information Technology

Domain: Cloud Infra & Security

Student ID: CT_CSI_CI_1160

Research & Development Document

CIDR Ranges of Azure VNet, Subnet, VNet Peering, and Use Case Deployment

---

Table of Contents

1. Introduction to Azure Virtual Network
2. CIDR Ranges: VNets and Subnets
3. Subnetting in Azure
4. VNet Peering and Its Types
5. Prerequisites for Deployment
6. Use Case:
    - Create VNet with Subnets
    - Deploy Windows & Linux VMs
    - Enable VM-to-VM Communication
    - Peer Two VNets and Enable Cross-Communication
7. Screenshots & Configuration Steps
8. Conclusion
9. Extended R&D: CIDR and Peering Concepts in Practice

1. Introduction to Azure Virtual Network (VNet)

An **Azure Virtual Network (VNet)** is a logically isolated network in Azure. It enables secure communication between Azure resources, the internet, and on-premises networks.

Key Features:

- Private IP address space using CIDR
- Subnet segmentation
- Network Security Groups (NSGs)
- Route tables
- VNet peering
- VPN Gateway & ExpressRoute support

2. CIDR Ranges in VNets and Subnets

CIDR (Classless Inter-Domain Routing) notation defines IP address ranges for VNets and subnets. CIDR allows the allocation of address blocks in a hierarchical, efficient manner.

Example:

- VNet CIDR: 10.0.0.0/16 → Contains 65,536 IP addresses
- Subnet 1: 10.0.1.0/24 → 256 IPs
- Subnet 2: 10.0.2.0/24 → 256 IPs

Azure reserves 5 IPs per subnet:

- Network address
- Broadcast address (reserved)

- First 3 usable IPs (reserved for Azure services)

CIDR Notation Table:

CIDR	Total IPs	Usable IPs
/24	256	251
/25	128	123
/26	64	59
/27	32	27
/28	16	11

3. Subnetting in Azure

Subnets allow segmentation of the VNet to apply policies (e.g., NSGs, UDRs) at subnet level. They enable:

- Logical isolation
- Role separation (e.g., Web, App, DB tiers)
- Granular control over traffic flow and IP ranges
- Load balancing and firewall targeting at subnet level

Recommended to use /24 or /26 for small environments. Subnets must not overlap.

4. VNet Peering in Azure

VNet Peering connects two VNets and allows communication through private IPs.

Types of Peering:

1. **Intra-region Peering** – VNets in the same Azure region
2. **Global VNet Peering** – VNets in different Azure regions

Benefits:

- Low-latency, high-bandwidth connectivity
- Private and secure communication
- No public internet exposure
- Shared services like DNS, Azure Bastion

Limitations:

- Transitive peering is **not supported** (i.e., VNet A peered to B, B to C doesn't mean A can talk to C)
- Cannot use overlapping address spaces

5. Prerequisites to Create VNets and VMs

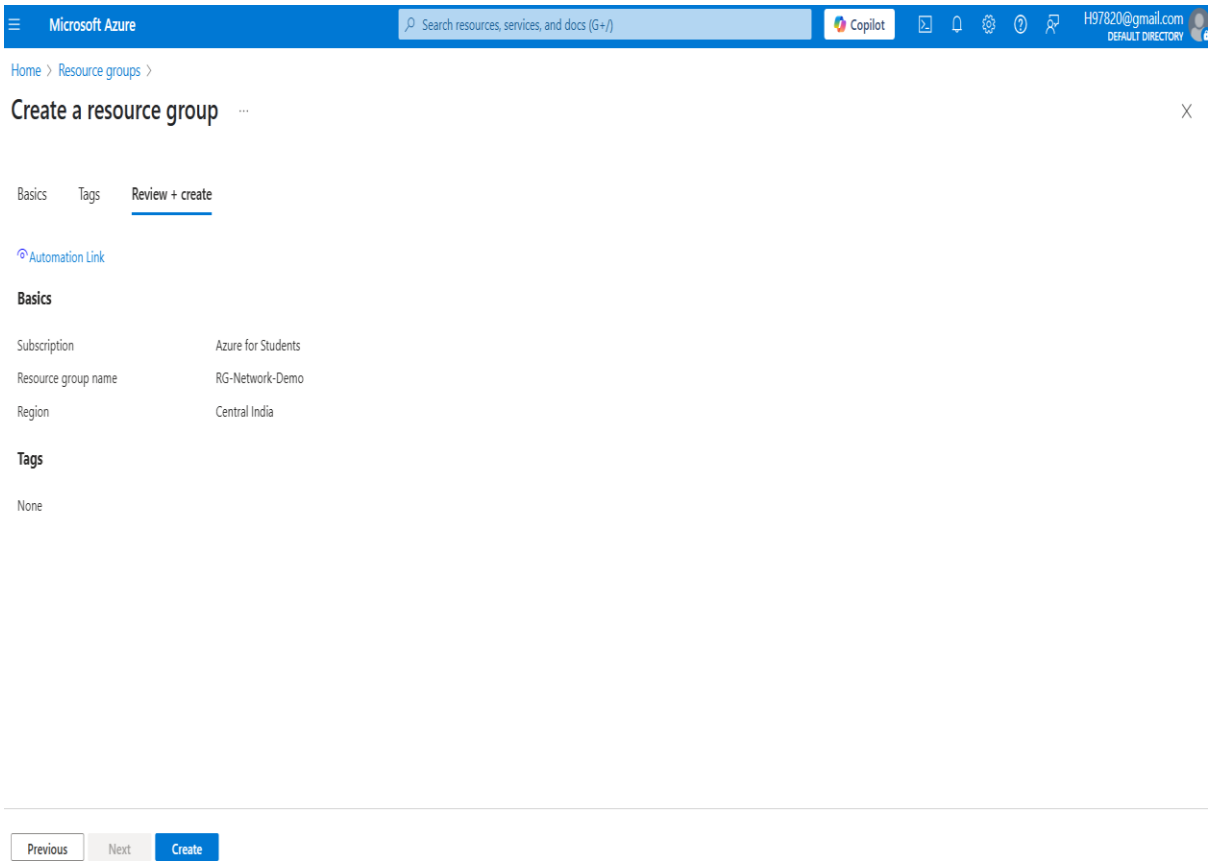
- Active Azure Subscription
- Resource Group created
- Understanding of IP/CIDR ranges
- Azure Portal access
- Basic networking knowledge (IP, ping, routing)
- Admin credentials for deploying VMs

6. Use Case: Deploying VNets, Subnets, VMs, and Peering

Objective: Create a virtual network setup with multiple subnets, deploy Windows and Linux VMs in separate subnets, test connectivity, and peer two VNets to demonstrate cross-network communication.

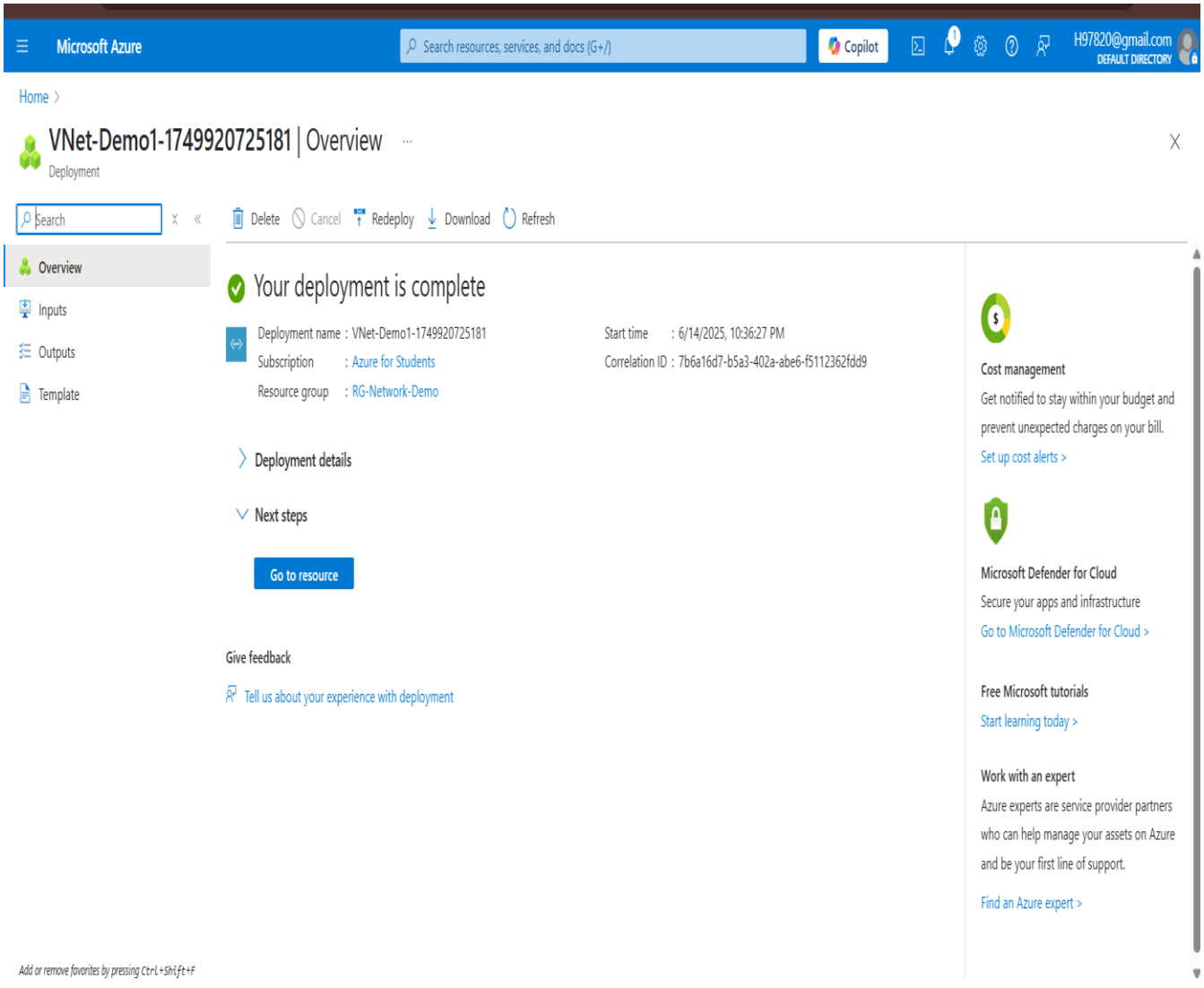
6.1 Step 1: Create Resource Group

- Azure Portal → Search "Resource groups"
- Click + Create
- Resource Group Name: RG-Network-Demo
- Region: Central India
- Click Review + Create → Create



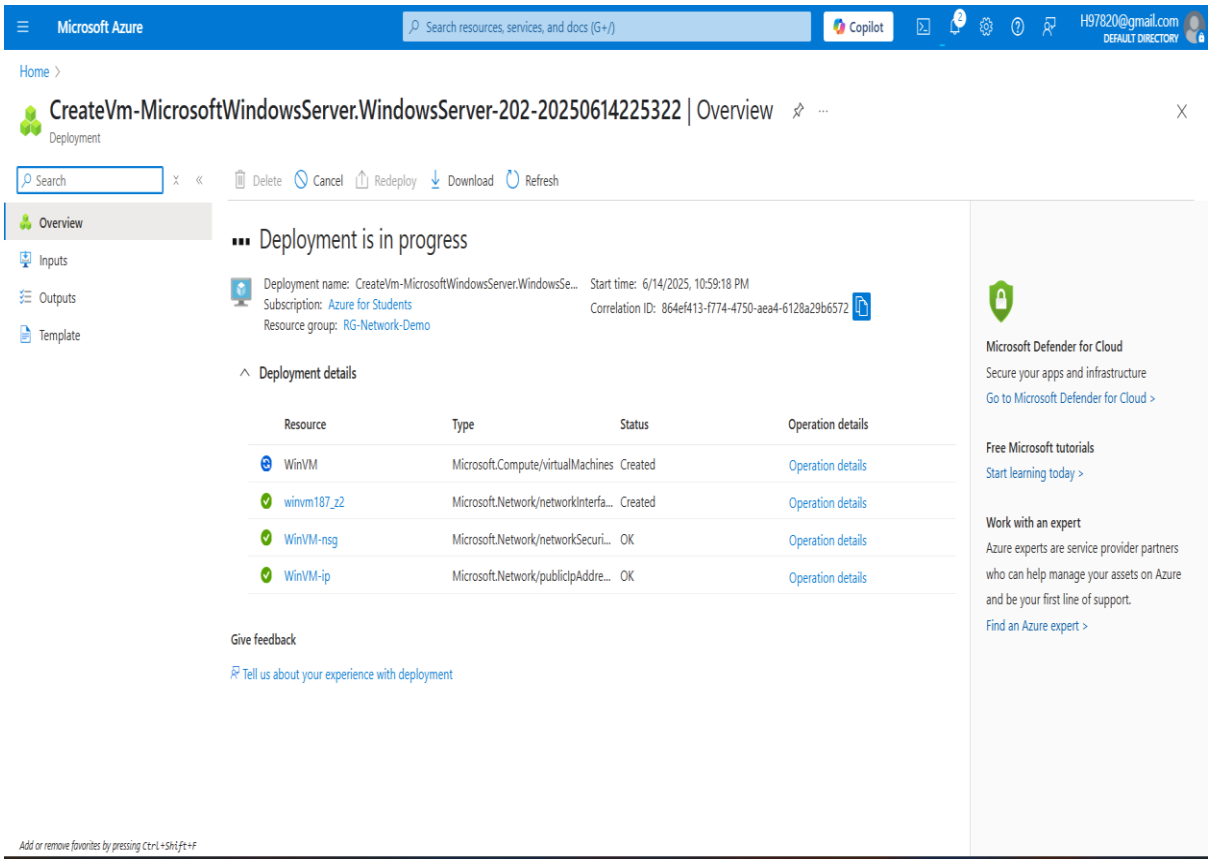
6.2 Step 2: Create First VNet and Subnets

- Azure Portal → "Virtual Networks" → + Create
- Name: VNet-Demo1
- Region: Central India
- Address space: 10.1.0.0/16
- Add Subnet 1: Subnet-Win → 10.1.1.0/24
- Add Subnet 2: Subnet-Linux → 10.1.2.0/24
- Click Review + Create → Create



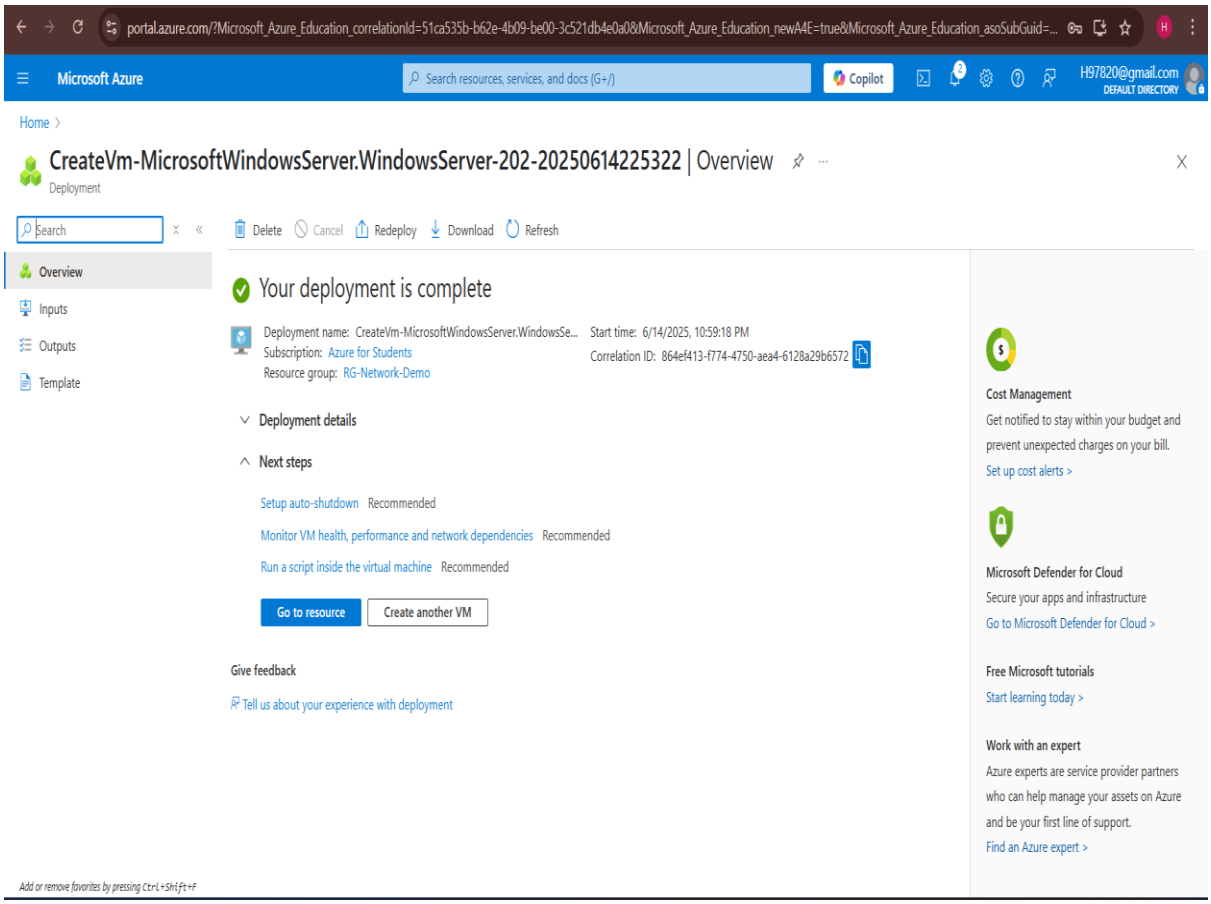
6.3 Step 3: Deploy Windows VM

- Azure Portal → "Virtual Machines" → + Create
- Name: WinVM
- Image: Windows Server 2022
- Region: Central India
- VNet: VNet-Demo1, Subnet: Subnet-Win
- Public IP: Enabled
- Inbound port: Allow RDP (3389)
- Set admin credentials
- Availability Zone: Set to Zone 2 if Zone 1 is not available
- Click Review + Create → Create



6.4 Step 4: Deploy Linux VM

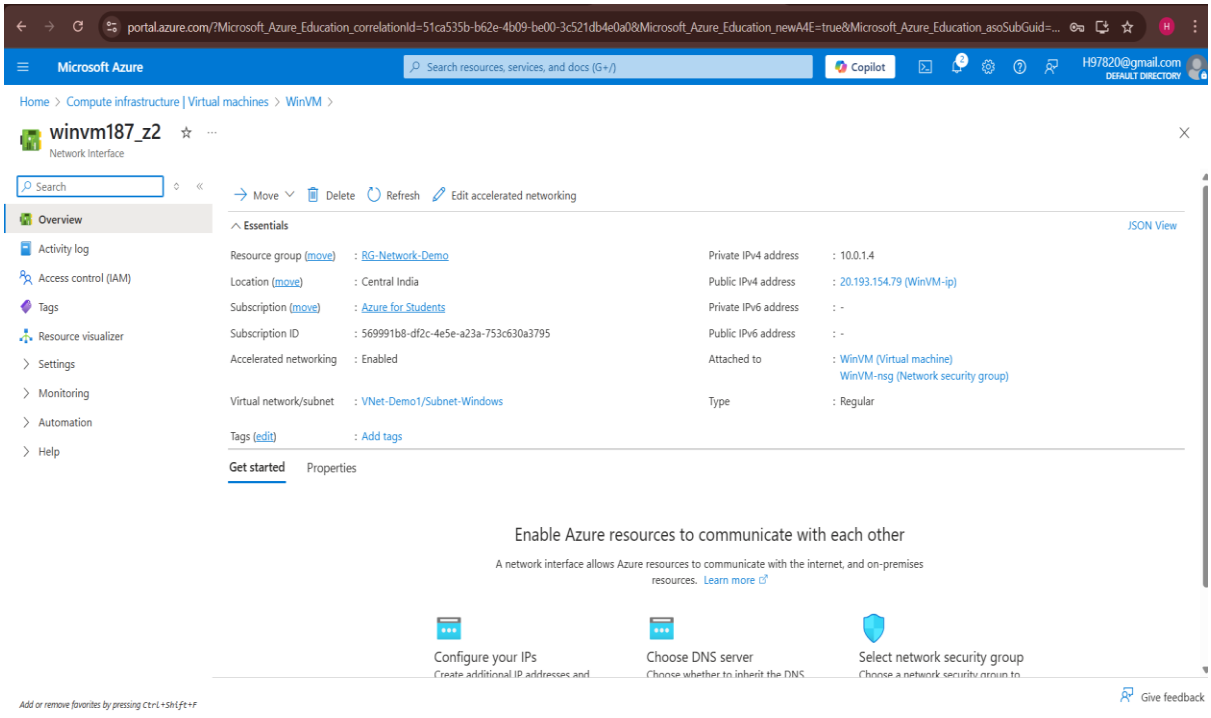
- Name: LinuxVM
- Image: Ubuntu 22.04 LTS
- Region: Central India
- VNet: VNet-Demo1, Subnet: Subnet-Linux
- Public IP: Enabled
- Inbound port: Allow SSH (22)
- Use SSH key or password
- Availability Zone: Set to Zone 2
- Click Review + Create → Create



6.5 Step 5: Enable Ping (ICMP) Between VMs

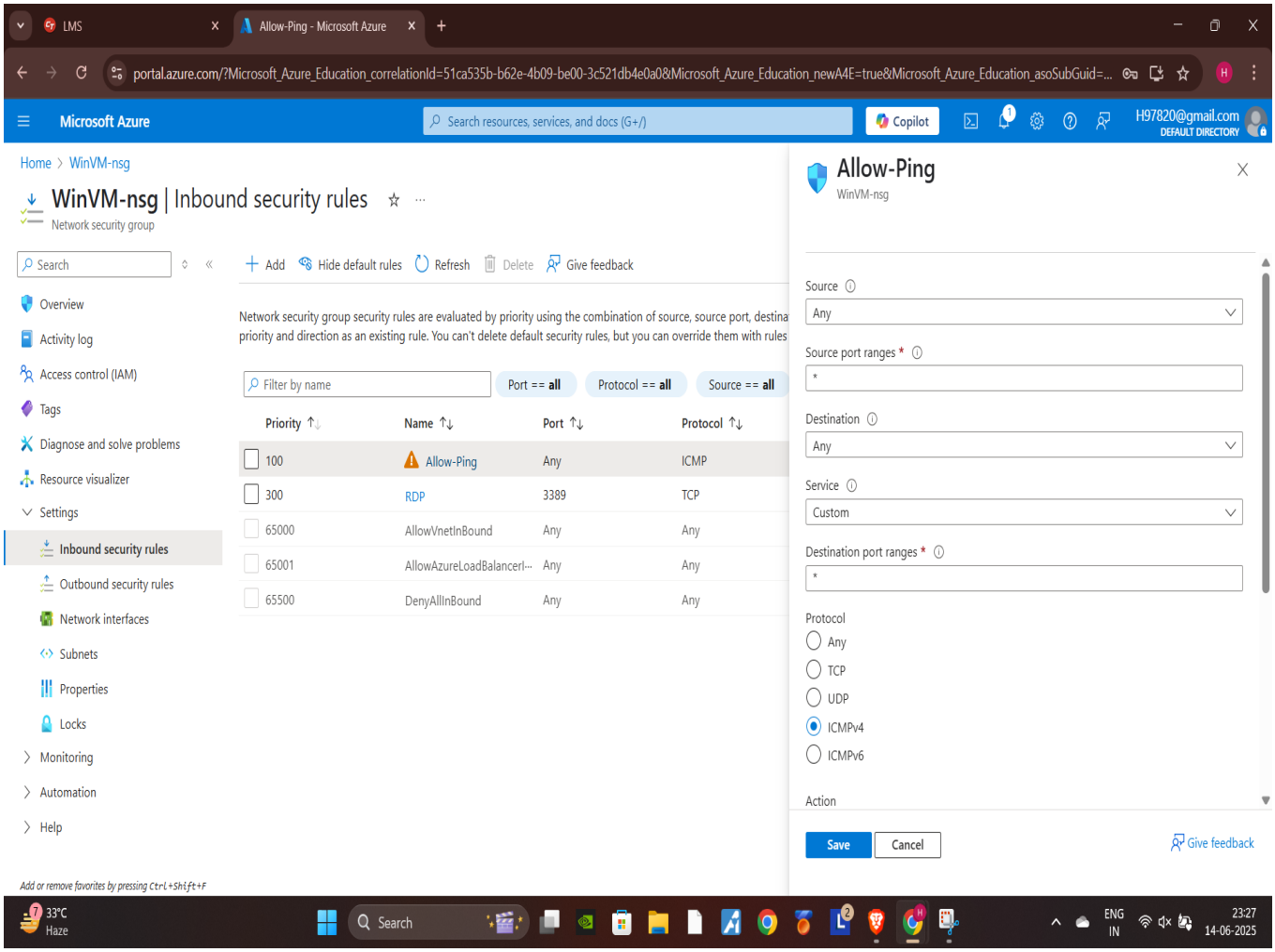
- Go to NSG linked with each VM NIC or subnet
- Add Inbound Rule:
    - Source: Any
    - Protocol: ICMP
    - Action: Allow
    - Priority: 100
    - Name: AllowPing
- **Connect to VMs**:
    - RDP into WinVM → Open Command Prompt → ping <LinuxVM Private IP>
    - SSH into LinuxVM → Run ping <WinVM Private IP>

If replies are received, VMs can communicate.



6.6 Step 6: Create Second VNet (VNet-Demo2)

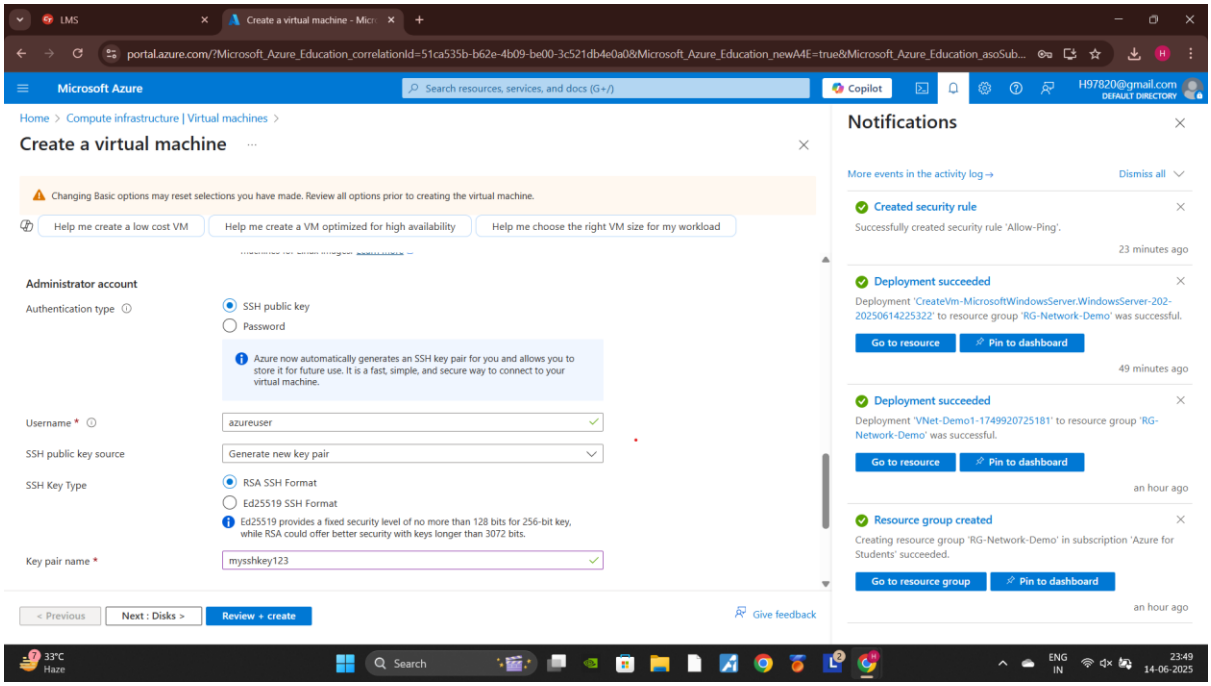
- Go to "Virtual Networks" → + Create
- Name: VNet-Demo2
- Region: Central India (or another)
- Address space: 10.2.0.0/16
- Subnet: Subnet-Peer → 10.2.1.0/24
- Click Review + Create → Create

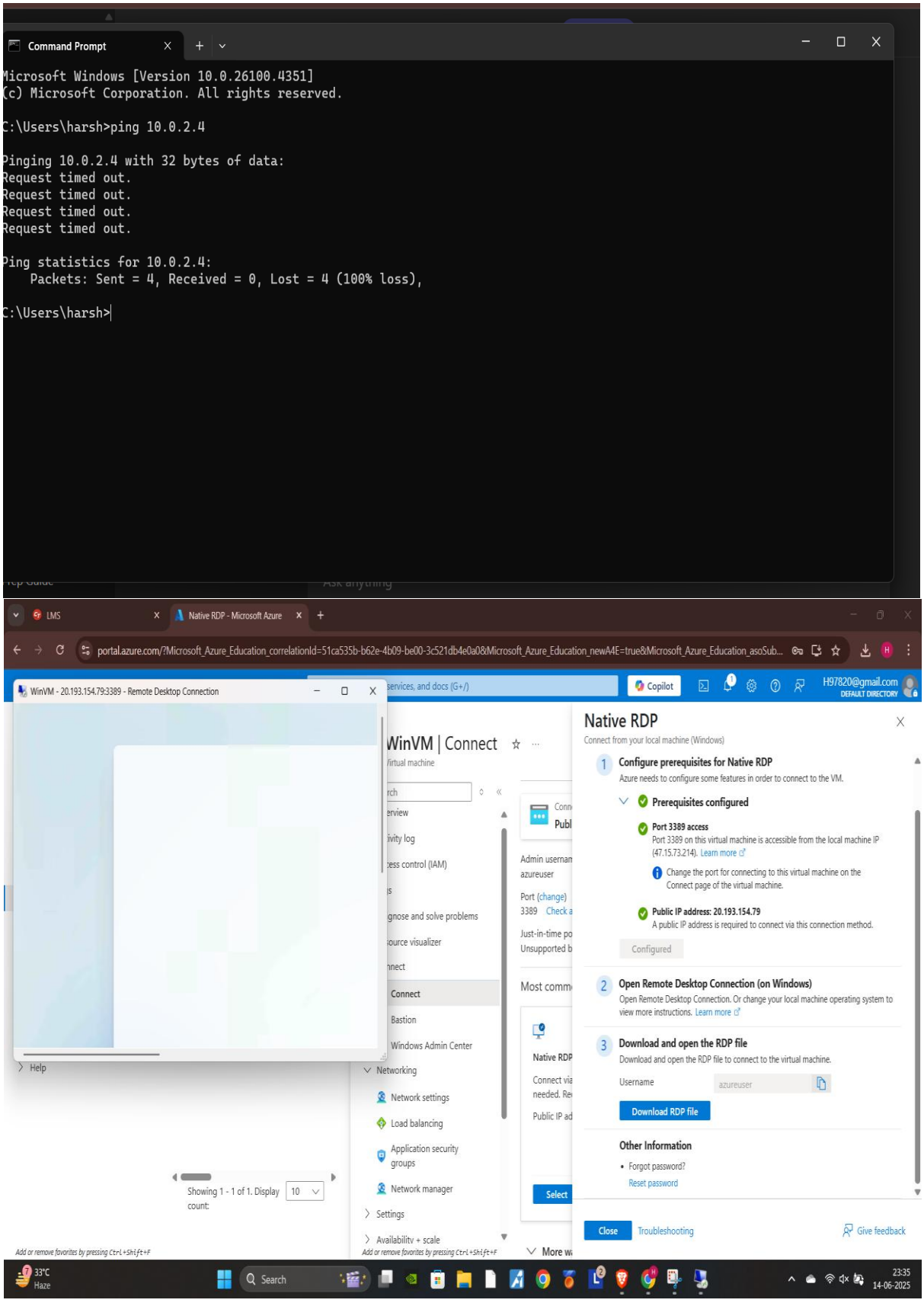


6.7 Step 7: VNet Peering Between VNet-Demo1 and VNet-Demo2

1. Go to VNet-Demo1 → Peerings → + Add
    - Name: peer-to-VNet2
    - Remote VNet: VNet-Demo2
    - Allow traffic in both directions: Yes
2. Go to VNet-Demo2 → Peerings → + Add
    - Name: peer-to-VNet1
    - Remote VNet: VNet-Demo1
    - Allow traffic in both directions: Yes

VMs in both VNets can now communicate via private IPs (check ICMP rules in NSGs).




Command Prompt
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.
C:\Users\harsh>ping 10.0.2.4
Pinging 10.0.2.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.2.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\harsh>
LMS
Native RDP - Microsoft Azure
WinVM - 20.193.154.79:3389 - Remote Desktop Connection
WinVM | Connect
Native RDP
Connect from your local machine (Windows)
1 Configure prerequisites for Native RDP
Azure needs to configure some features in order to connect to the VM.
Prerequisites configured
Port 3389 access
Port 3389 on this virtual machine is accessible from the local machine IP (47.15.73.214). Learn more
Change the port for connecting to this virtual machine on the Connect page of the virtual machine.
Public IP address: 20.193.154.79
A public IP address is required to connect via this connection method.
Configured
2 Open Remote Desktop Connection (on Windows)
Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. Learn more
3 Download and open the RDP file
Download and open the RDP file to connect to the virtual machine.
Username
azureuser
Download RDP file
Other Information
Forgot password?
Reset password
Close
Troubleshooting
Give feedback
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Connect
Bastion
Windows Admin Center
Help
Search
33°C
Haze
23:35
14-06-2025

8. Conclusion

This document demonstrates the step-by-step process of:

- Defining CIDR ranges in VNets and Subnets
- Creating logically segmented subnets
- Deploying Windows and Linux VMs
- Enabling communication within a VNet
- Establishing secure VNet Peering across networks

The implementation ensures secure and scalable network communication architecture on Azure.

9. Extended R&D: CIDR and Peering Concepts in Practice

- CIDR is essential for efficient IP allocation in cloud networking. Larger CIDR blocks (e.g., /16) are allocated to VNets to allow further subnetting as needs grow.
- Subnetting strategies differ for production vs. dev/test environments.
- Peering reduces the need for VPN gateways when VNets are within the same tenant.
- Azure recommends peering instead of routing through a hub VNet unless using NVAs (network virtual appliances).
- IP overlap issues are common in large environments—always design IP plans before creating VNets.
