# R&D Report on CIDR Ranges, VNets, Subnets, and VNet Peering

Prepared by:
Virat Pandey

Celebal Technology
Cloud Infrastructure & Security Internship

Research & Development Document

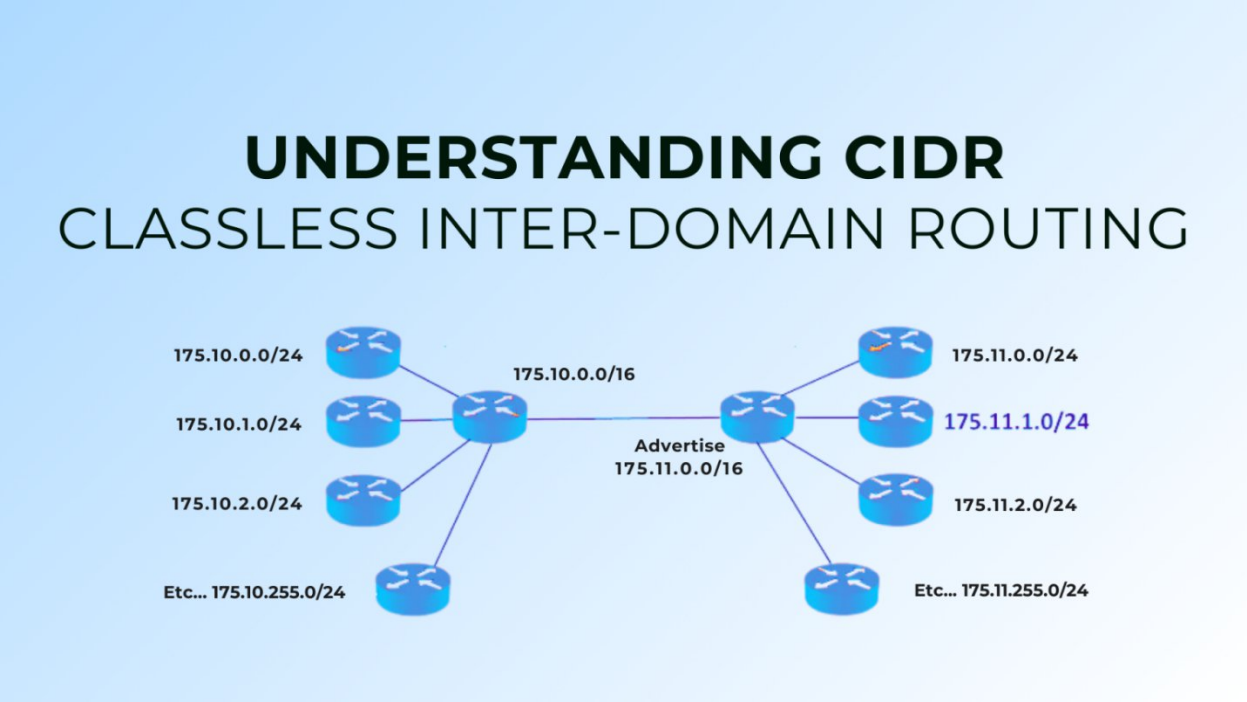
25 June , 2025

# Table of contents

# 1. Introduction

As cloud networking becomes the backbone of modern infrastructure, it is essential to understand how networks are logically designed and interconnected. Microsoft Azure offers **Virtual Networks (VNets)** to securely connect Azure resources, define IP spaces, and manage network segmentation through **subnets**. These VNets are built using **CIDR (Classless Inter-Domain Routing)** blocks, allowing flexible and hierarchical IP address planning.

Additionally, Azure enables secure communication between VNets through **VNet Peering**, which allows direct traffic flow between networks without the need for a VPN gateway. Peering can be established across regions or within the same region, supporting various enterprise-grade networking scenarios.
This report explores the fundamental concepts behind CIDR notation, VNets, subnets, and peering mechanisms — serving as both a conceptual foundation and practical reference for deploying scalable, secure, and efficient network architectures on Azure.



## 2. Understanding CIDR Ranges

**CIDR (Classless Inter-Domain Routing)** is a method used to allocate IP addresses and route IP packets efficiently. Unlike traditional IP address classes (Class A, B, C), CIDR allows for **more granular and flexible subnetting** using variable-length subnet masks (VLSM).

In CIDR notation, an IP address is followed by a **slash ( / ) and a number** indicating how many bits are used for the network portion. The remaining bits are used for host addresses within that network.

**Example:**

- **CIDR Notation:** 10.0.0.0/16
- **Network Portion:** First 16 bits
- **Available Host Bits:** Remaining 16 bits
- **Usable IPs:** 65,534 ($2^{16} – 2$)

◆ **Why CIDR Is Important in Azure:**

In Azure, when you create a Virtual Network (VNet), you must specify a **CIDR range** to define the overall IP address space. This range is then divided into **subnets**, each with their own CIDR blocks.

- Prevents **IP conflicts**
- Supports **efficient use of IP space**
- Enables **custom subnetting strategies** for tiered applications

| CIDR | **Total IPs** | **Usable Hosts** | **Common Use** |
|---|---|---|---|
| /2<br>4 | 25<br>6 | 25<br>4 | Small subnet (VMs, pods) |

| | | | |
|---|---|---|---|
| /22 | 1024 | 1022 | Medium workloads |
| /16 | 65,536 | 65,534 | Large VNets or address pool |
| /30 | 4 | 2 | Point-to-point networking |

## 3. Azure Virtual Networks (VNets).

A **Virtual Network (VNet)** in Azure is a logically isolated section of the cloud dedicated to your subscription. It enables Azure resources such as virtual machines, databases, and applications to securely communicate with each other, the internet, and on-premises environments.

VNets provide the **foundation for Azure networking**, functioning similarly to traditional on-premises networks but with added flexibility, scalability, and integration with other Azure services.

- **Key Features of Azure VNets:**
  - **Custom IP Address Space:**
    When creating a VNet, you define its IP range using CIDR notation (e.g., 10.0.0.0/16).

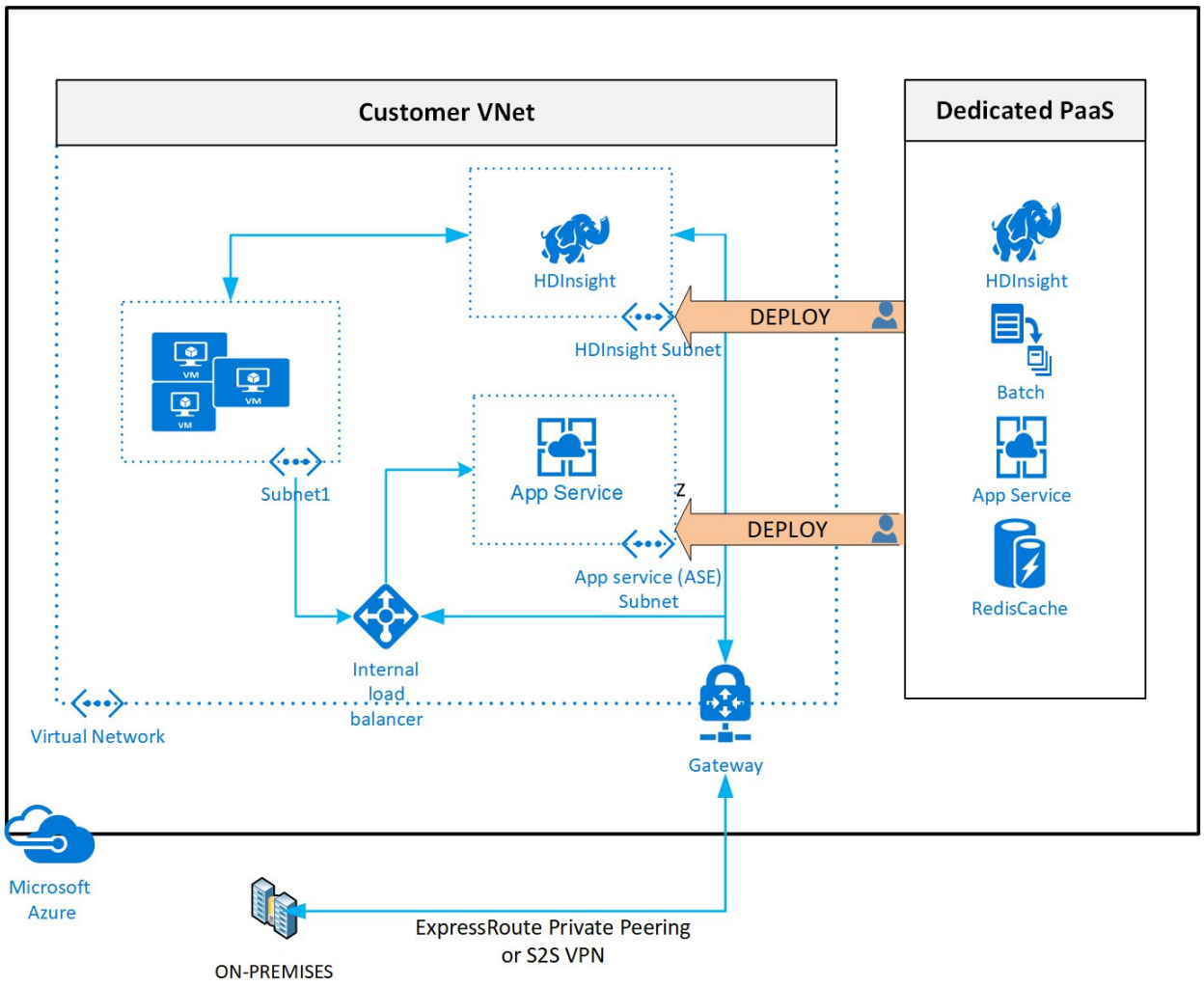
- **Subnets for Segmentation:**
  VNets can be divided into smaller segments (subnets) for isolating workloads (e.g., web, app, database tiers).
- **Region-Specific:**
  VNets are scoped to a specific Azure region but can connect across regions via peering.
- **Secure Communication:**
  Built-in support for **NSGs (Network Security Groups)**, **firewalls**, **route tables**, and **service endpoints**.
- **Hybrid Connectivity:**
  VNets can connect to on-premises networks via **VPN gateways** or **ExpressRoute** for hybrid cloud setups.

📌 **Example Use Case:**

A company deploying a 3-tier web application might create a single VNet with three subnets:

- 10.0.1.0/24 for the Web tier
- 10.0.2.0/24 for the Application tier
- 10.0.3.0/24 for the Database tier

This allows them to apply specific NSG rules to each tier while keeping all traffic within the same isolated virtual network.




**Virtual Networks in Azure offer the building blocks for designing secure, scalable, and logically segmented cloud networks.” — Microsoft Learn [2]**

# 4. Subnets in Azure and Address Allocation.

Once a Virtual Network (VNet) is created in Azure, it is **divided into smaller segments called subnets**, which allow better **organization, isolation, and control** over network resources. Each subnet represents a **logical subdivision** of the VNet's IP space and is assigned its own **CIDR block**.
Subnets play a crucial role in organizing services by tier (such as web, application, and database), applying **network security policies**, and managing **traffic flow** within and across networks.

- **Key Concepts:**
  - **Subnet Address Range:**
    Each subnet is assigned a **unique, non-overlapping CIDR range** from the VNet's overall address space.
  - **Routing:**
    Azure automatically sets up **system routes** for traffic between subnets in the same VNet. Custom routes can also be added.
  - **NSGs (Network Security Groups):**
    You can associate NSGs with subnets to control inbound/outbound traffic using **ACL rules**.
  - **Service Delegation & Endpoints:**
    Subnets can be delegated to specific Azure services (like Azure SQL, Cosmos DB) or connected to services using **service endpoints**.
  - **Subnet-to-Subnet Communication:**
    By default, all subnets in the same VNet can communicate with each other. You can restrict this using NSGs or route tables.

| Subnet Name | CIDR Range | Purpose |
|---|---|---|
| Web-Subnet | 10.1.1.0/24 | Hosts web servers |
| App-Subnet | 10.1.2.0/24 | Hosts backend APIs |
| DB-Subnet | 10.1.3.0/24 | Hosts SQL database |

This allows each tier to have independent **security policies**, **routing rules**, and **resource allocation**.
“Subnetting in Azure enables fine-grained control over traffic, security, and service behavior — critical for designing scalable and secure environments.” — Microsoft Learn [3]

## 5. VNet Peering and Its Types

**VNet Peering** is a feature in Azure that allows **direct, high-speed, low-latency communication** between two virtual networks (VNets), either within the same region or across different Azure regions. It connects VNets using Azure's backbone infrastructure without requiring public internet, VPN, or gateways.
VNet peering enables organizations to scale their architecture, segment environments (e.g., dev, test, prod), and maintain security while ensuring seamless network integration.

- **Key Benefits of VNet Peering:**
  - **No bandwidth bottlenecks** — uses Azure’s high-speed internal network
  - **Low latency** — ideal for high-performance workloads across VNets
  - **Secure communication** — traffic stays within Azure, not over the internet
  - **Transitive routing support** (with limitations and careful design)
  - **No downtime** — peering connections are established instantly

### 5.1 Intra-Region VNet Peering

This type of peering connects two VNets **in the same Azure region**.

**Example:**

Connect VNet-Dev (10.1.0.0/16) and VNet-Test (10.2.0.0/16) — both located in **Central India**.

Use cases:

- Segmenting workloads by function (e.g., Web and DB)
- Connecting VNets managed by different teams or departments

## 5.2 Global VNet Peering

This allows VNets in **different Azure regions** to be connected (e.g., India ↔ East US).

**Example:**

VNet-India (10.1.0.0/16) in **Central India** and VNet-US (10.3.0.0/16) in **East US**.

Use cases:

- Multi-region deployments for global applications
- Disaster recovery and geographic redundancy

Note: Bandwidth charges apply for cross-region data transfer.

## 5.3 Key Differences and Considerations

| Feature | Intra-Region Peering | Global VNet Peering |
|---|---|---|
| Same region | ✔ | ✖ |
| Across regions | ✖ | ✔ |
| Latency | Very Low | Slightly higher |
| Cost for data transfer | Free within same region | Billed per GB transferred |
| Gateway required | ✖ | ✖ |
| Use Azure backbone? | ✔ | ✔ |

# 6. CIDR Planning Best Practices in Azure

Proper **CIDR planning** is critical when designing Azure Virtual Networks and subnets. A well-structured IP addressing plan ensures smooth network scalability, avoids overlaps, and simplifies management — especially when peering multiple VNets or integrating with on-premises systems.

- **Key CIDR Planning Guidelines:**

1. **Start with a Broad IP Range (VNet-level):**
   Always reserve a large enough address space for your VNet (e.g., /16), even if you're starting with only a few subnets. This allows room for future expansion.
   - ✅ Example: Use 10.0.0.0/16 for the VNet
   - Then divide into /24 or /26 subnets as needed
2. **Avoid Overlapping IP Ranges:**
   Overlapping CIDR blocks can break **VNet peering**, **VPN connections**, or **hybrid integrations**. Always plan non-overlapping ranges between VNets and subnets.
3. **Allocate Subnets by Function/Tier:**
   Assign subnets logically based on workload roles:
   - 10.0.1.0/24 – Web Tier
   - 10.0.2.0/24 – App Tier
   - 10.0.3.0/24 – Database Tier
4. **Reserve Space for Future Subnets:**
   Avoid filling your CIDR range completely. Leave gaps for future additions like private endpoints, VPN gateways, Bastion hosts, etc.
5. **Document Your IP Plan:**
   Maintain a central document or spreadsheet for your team listing:
   - VNet names and their CIDR blocks
   - Subnet names, roles, and CIDRs
   - Notes on peering or reserved IPs
6. **Align With RFC 1918 Address Space:**
   Use private IP address ranges recommended for internal use:
   - 10.0.0.0/8

- 172.16.0.0/12
- 192.168.0.0/16

| Component | CIDR Range | Purpose |
|---|---|---|
| VNet-Main | 10.10.0.0/16 | Primary network |
| Subnet-Web | 10.10.1.0/24 | Web servers |
| Subnet-App | 10.10.2.0/24 | Application servers |
| Subnet-DB | 10.10.3.0/24 | Database servers |
| Reserved for future | 10.10.4.0/24 | Private endpoints / growth |

## 7. Conclusion

Understanding and applying CIDR ranges, VNets, subnets, and VNet peering is fundamental to designing scalable, secure, and efficient cloud network architectures in Microsoft Azure. These elements form the backbone of all Azure-based deployments, from simple two-VM setups to large, multi-region enterprise environments.
CIDR enables flexible IP address allocation, allowing organizations to tailor networks to their specific needs without wasting address space. Subnets provide logical segmentation within VNets, facilitating traffic control and layered security. VNet peering—both intra-region and global—empowers seamless, low-latency communication between VNets without the complexity of traditional VPN gateways.
When used together, these features support modern cloud architecture principles: modularity, isolation, scalability, and high availability. Whether you're building a single-tier app or a globally distributed solution, proper planning and implementation of Azure networking services ensure robust performance and long-term maintainability.

## 8. Reference

1. Microsoft. (2024). *Azure Virtual Network FAQ*. Explains CIDR ranges, subnet size limits, and non-overlapping requirements learn.microsoft.comlearn.microsoft.com+6learn.microsoft.com+6learn.microsoft.com+6
2. Microsoft. (2025). *Add, change, or delete a subnet*. Guides on subnet configuration, CIDR notation, and portal steps learn.microsoft.com
3. Microsoft. (2025). *Virtual network peering overview*. Details intra-region vs. global peering, latency, and bandwidth characteristics learn.microsoft.com+11learn.microsoft.com+11learn.microsoft.com+11
4. Microsoft. (2025). *Create, change, or delete Azure virtual network peering*. Step-by-step instructions for portal, CLI, and PowerShell learn.microsoft.com+13learn.microsoft.com+13learn.microsoft.com+13
5. Microsoft. (2025). *Concepts and best practices for virtual network*. Recommendations on CIDR planning, subnetting, and avoiding overlap learn.microsoft.com
6. Microsoft. (2024). *Plan for IP addressing - Cloud Adoption Framework*. Discusses CIDR use with preview of IPv4/IPv6 integration learn.microsoft.com