**Azure Hub-and-Spoke Network Architecture**

**Internship Final Project Report**

**Name: Kanishk Dwivedi  
University: Manipal University Jaipur  
Internship: Celebal Technologies – DevOps   
Date: 23rd July 2025**

**Objective:**

The goal of this project is to design and implement a secure and scalable cloud network using the **Hub-and-Spoke topology** on Microsoft Azure. The model ensures centralized routing, security enforcement, and seamless connectivity across multiple application environments.

A **Hub** Virtual Network (VNet) acts as a central control point, connected to multiple **Spoke VNets** (App and Dev environments) through **VNet peering**, while routing is controlled via **Azure Firewall**.

**Architecture Overview**

* Hub-VNet (10.0.0.0/16): Contains Azure Firewall and shared services.
* Spoke1: App-VNet (10.1.0.0/16): Hosts application workloads.
* Spoke2: Dev-VNet (10.2.0.0/16): Used for development/testing.
* VNet Peering: Enables controlled connectivity between Hub and Spokes.
* Azure Firewall: Central traffic inspection, NAT, and application rules.
* NSGs (Network Security Groups): Access control at subnet level.
* Network Watcher: For diagnostics, logging, and IP flow verification.

**Azure Services Used**

* Azure Virtual Networks (VNets)
* Subnets and VNet Peering
* Azure Firewall
* Network Security Groups (NSGs)
* Azure Virtual Machines (Linux and Windows)
* Azure Network Watcher
* IP Flow Verify and Connection Troubleshoot
* NSG Flow Logs & Diagnostic Settings

**Implementation Phases**

1. Phase 1: Create Hub-VNet with two subnets (FirewallSubnet and HubVMSubnet)
2. Phase 2: Create two Spoke VNets (App-VNet, Dev-VNet), configure peering to Hub
3. Phase 3: Deploy Azure Firewall in Hub, route traffic from spokes via Firewall
4. Phase 4: Validate routing and traffic flow using ping, DNS, and connection tests
5. Phase 5: Create and associate NSGs with subnet-specific rules (allow RDP/SSH, ICMP)
6. Phase 6: Enable Network Watcher, IP Flow, Connection Troubleshoot, and NSG Flow Logs

**Outcomes & Benefits**

* Centralized Network Security using Azure Firewall
* Controlled Access via NSGs and Peering configurations
* Spoke-to-Spoke Isolation for enhanced security
* Diagnostic Capabilities through Network Watcher and Flow Logs
* Production-Grade Design for scalable and maintainable enterprise environments

**Project Repository -**

GitHub: [github.com/kanishkdw/azure-hub-and-spoke-project](https://github.com/kanishkdw/azure-hub-and-spoke-project)  
Contains:

* README.md with instructions
* Folder for each phase (phase-1-setup, phase-2-vnet-peering, etc.)
* Commands used, screenshots, and markdown documentation