CSE 472: Cloud Computing Project Report

GROUP A5		
Name	ID	Role
Aqib Reza	1731085	Hands on Cloud configuration
Avijit Saha	1930109	Hands on Cloud configuration
Abu Bakar Siddique	1731237	Project Planning and background
Prantika Roy	2021040	Report writing and presentation
Sudipta Saha	2022664	Finding challenges and solutions

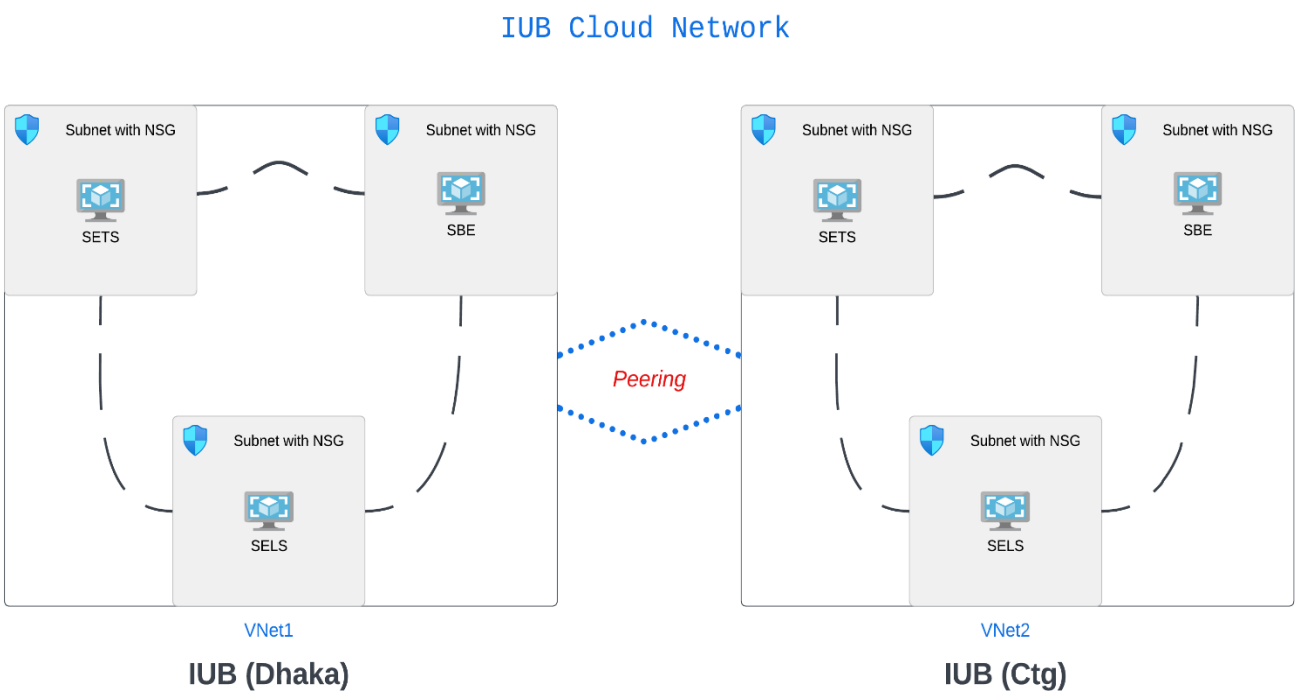
Project:
On Premises Network to Cloud Migration

Submitted to:
Dr. Rubaiyat Islam

Goal:

The goal of our project is to successfully migrate IUB's on-premises network to a cloud-based infrastructure, enabling us to leverage the benefits of cloud computing, such as scalability, cost optimization, and improved agility. The migration process will be planned and executed in a phased manner, ensuring minimal disruption to our operations and maintaining data security and compliance throughout the transition.

Network Diagram



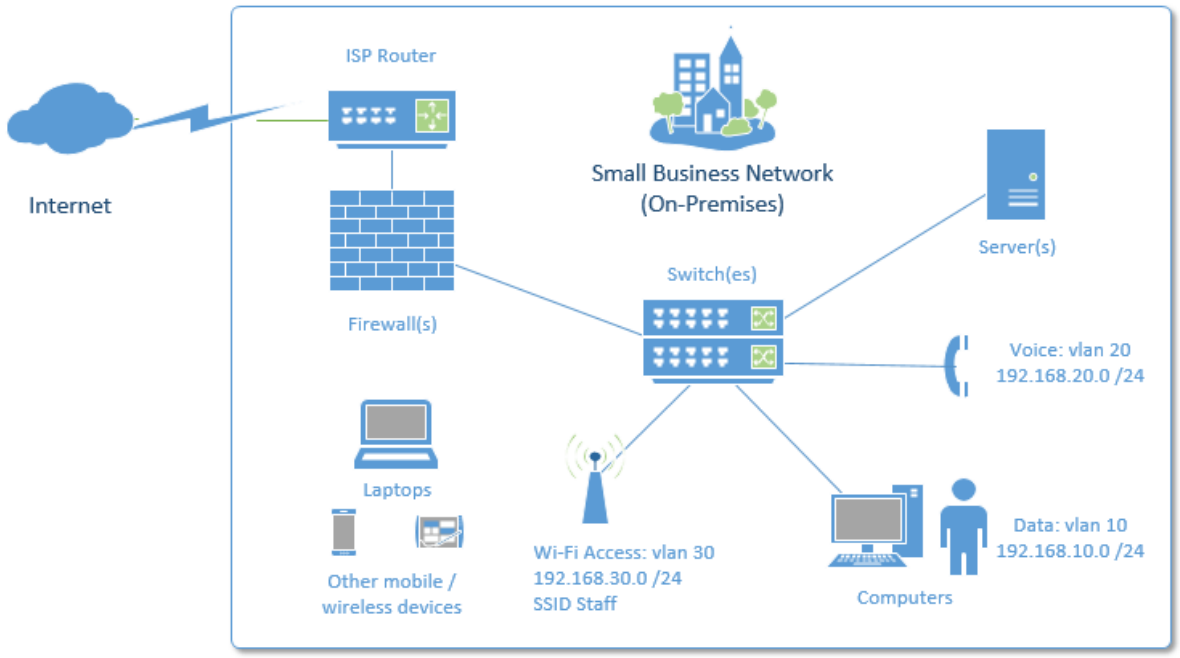
Preferred Cloud Platform:

After careful evaluation, research, and analysis, we have determined that Microsoft Azure is the most suitable cloud platform for our on-premises network to cloud migration project. So our main goal would be to create a network migration base on an azure environment.

On Premise Network and Cloud Networks Key Differences:

Migrating an on-premises network to Azure cloud network has both pros and cons, and the decision to migrate should be based on your specific business needs and requirements. Here are some of the specification on why an organization or company should choose on-premises network versus Azure cloud network.

On-Premises Network:



Positives:

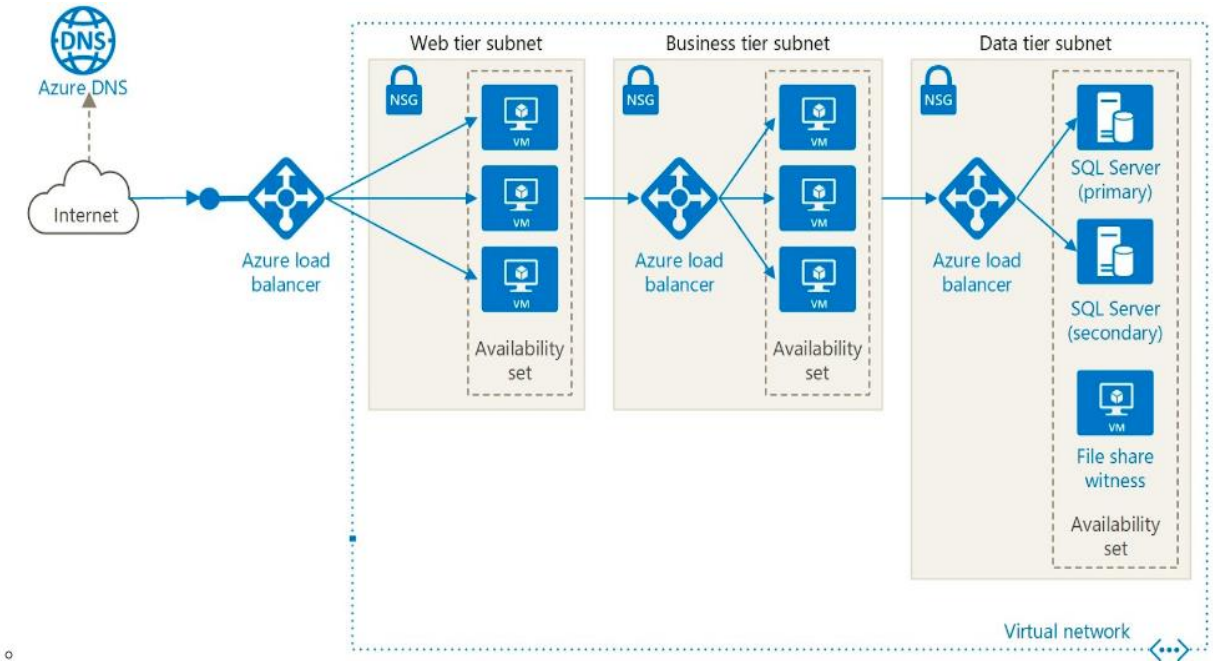
- Full control and ownership over the infrastructure
- Ability to customize and configure the network to meet specific business needs
- No reliance on third-party providers for network infrastructure
- Low latency and high-speed connectivity within the local network

Negatives:

- High upfront capital costs for hardware and infrastructure

- Ongoing maintenance and management costs
- Limited scalability and capacity to handle spikes in demand
- Requires skilled IT staff to manage and maintain the network

Azure Cloud Network:



Positives:

- Lower upfront costs as the infrastructure is provided by Microsoft
- Highly scalable to meet varying demands and workloads
- No ongoing maintenance or management costs for the underlying infrastructure
- Highly available and fault-tolerant architecture
- Offers a wide range of services and tools to meet different business needs

Negatives:

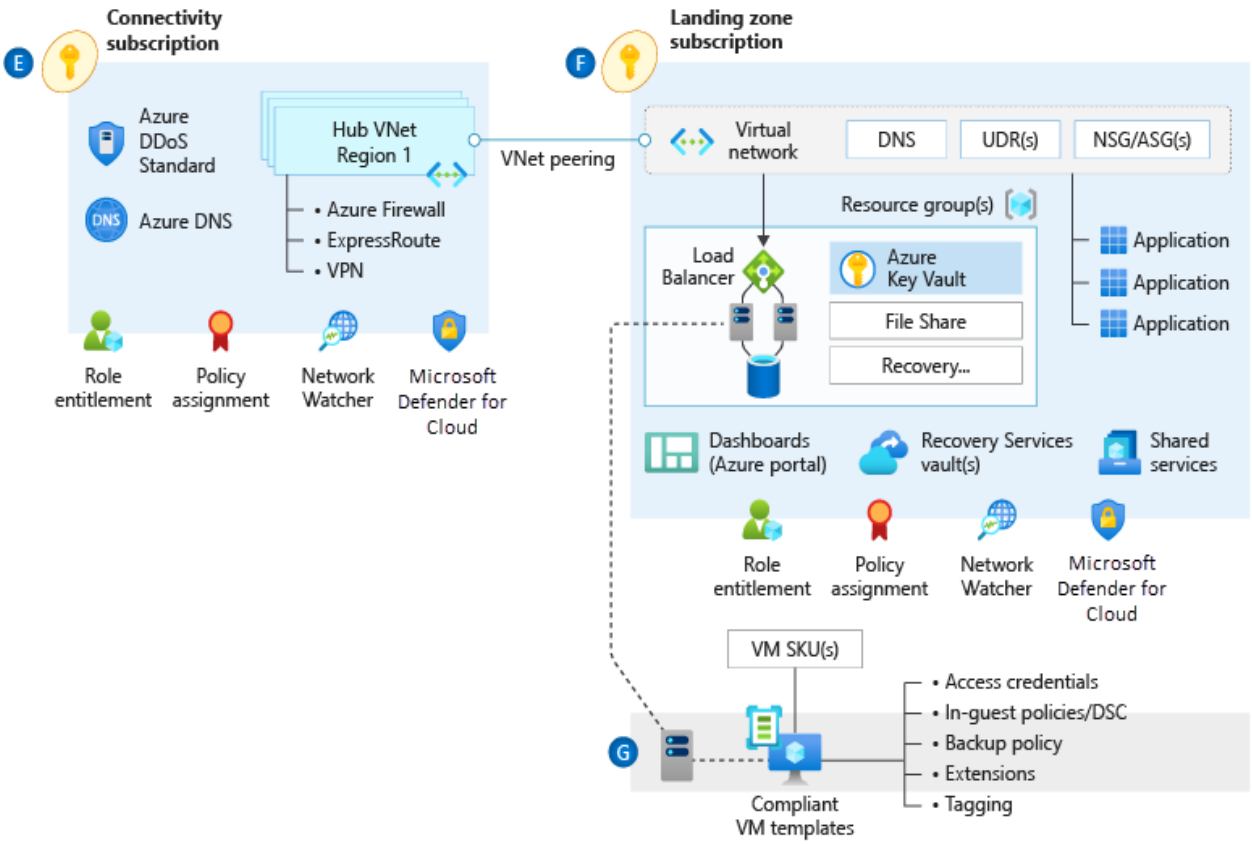
- Requires reliance on Microsoft for network infrastructure and services
- Possible latency and performance issues due to the internet connection

- Limited control over the infrastructure compared to an on-premises network
- Need to ensure compliance and security of data stored in the cloud

Overall, migrating to an Azure cloud network can offer many benefits, including scalability, cost savings, and a wide range of services and tools. However, it's important to carefully consider the potential drawbacks and ensure that migrating to the cloud aligns with your specific business needs and requirements.

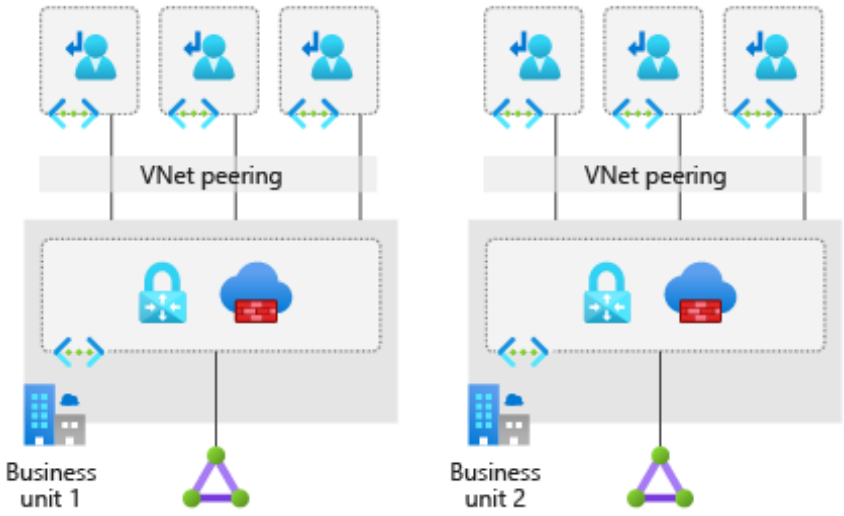
Azure Network Topology:

Network topology is a critical element of the landing zone architecture because it defines how applications can communicate with each other. This section explores technologies and topology approaches for Azure deployments. It focuses on two core approaches: topologies based on Azure Virtual WAN, and traditional topologies.

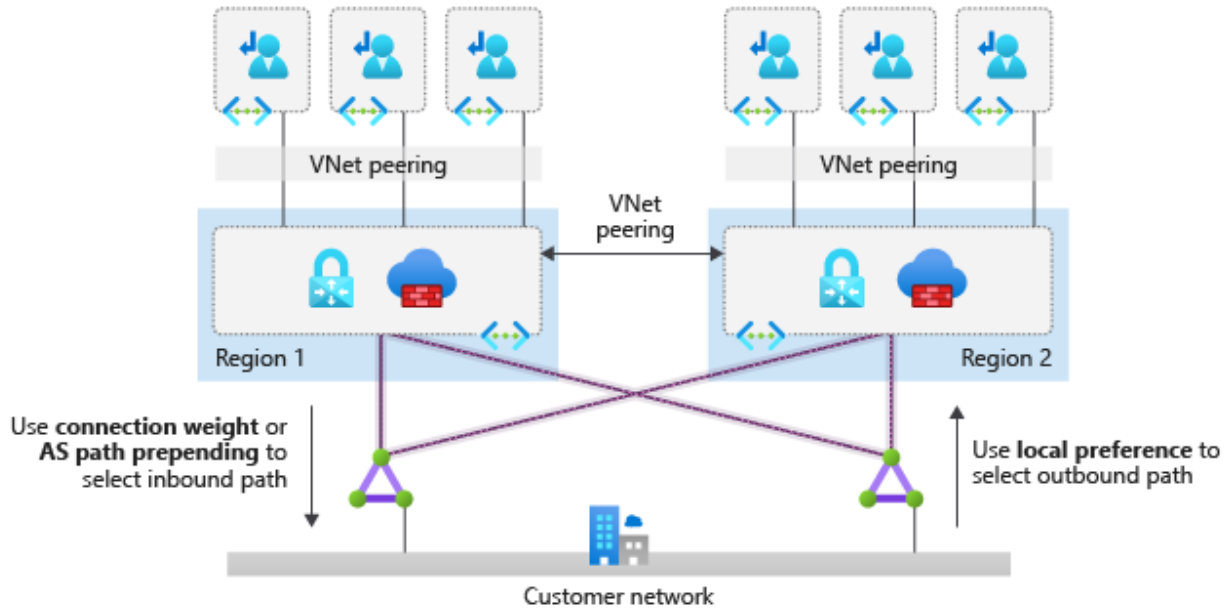


Various network topologies can connect multiple landing zone virtual networks. Examples of network topologies include one large flat virtual network, multiple virtual networks connected with multiple Azure ExpressRoute circuits or connections, hub-and-spoke, full mesh, and hybrid. Virtual networks can't traverse subscription boundaries. However, you can achieve connectivity between virtual networks across different subscriptions by using virtual network peering, an ExpressRoute circuit, or VPN gateways. Virtual network peering is the preferred method to connect virtual networks in Azure. You can use virtual network peering to connect virtual networks in the same region, across different Azure regions, and across different Azure Active Directory (Azure AD) tenants. Virtual network peering and global virtual network peering aren't transitive. To enable a transit network, you need user-defined routes (UDRs) and network virtual appliances (NVAs). For more information, see Hub-spoke network topology in Azure.

You can share an Azure DDoS Protection plan across all virtual networks in a single Azure AD tenant to protect resources with public IP addresses. For more information, see Azure DDoS Protection. Azure DDoS Protection plans cover only resources with public IP addresses. The cost of an Azure DDoS Protection plan includes 100 public IP addresses across all protected virtual networks associated with the DDoS Protection plan. Protection for more resources is available at a separate cost. For more information on Azure DDoS Protection plan pricing, see the Azure DDoS Protection pricing page or the FAQ. Review the supported resources of Azure DDoS Protection plans.



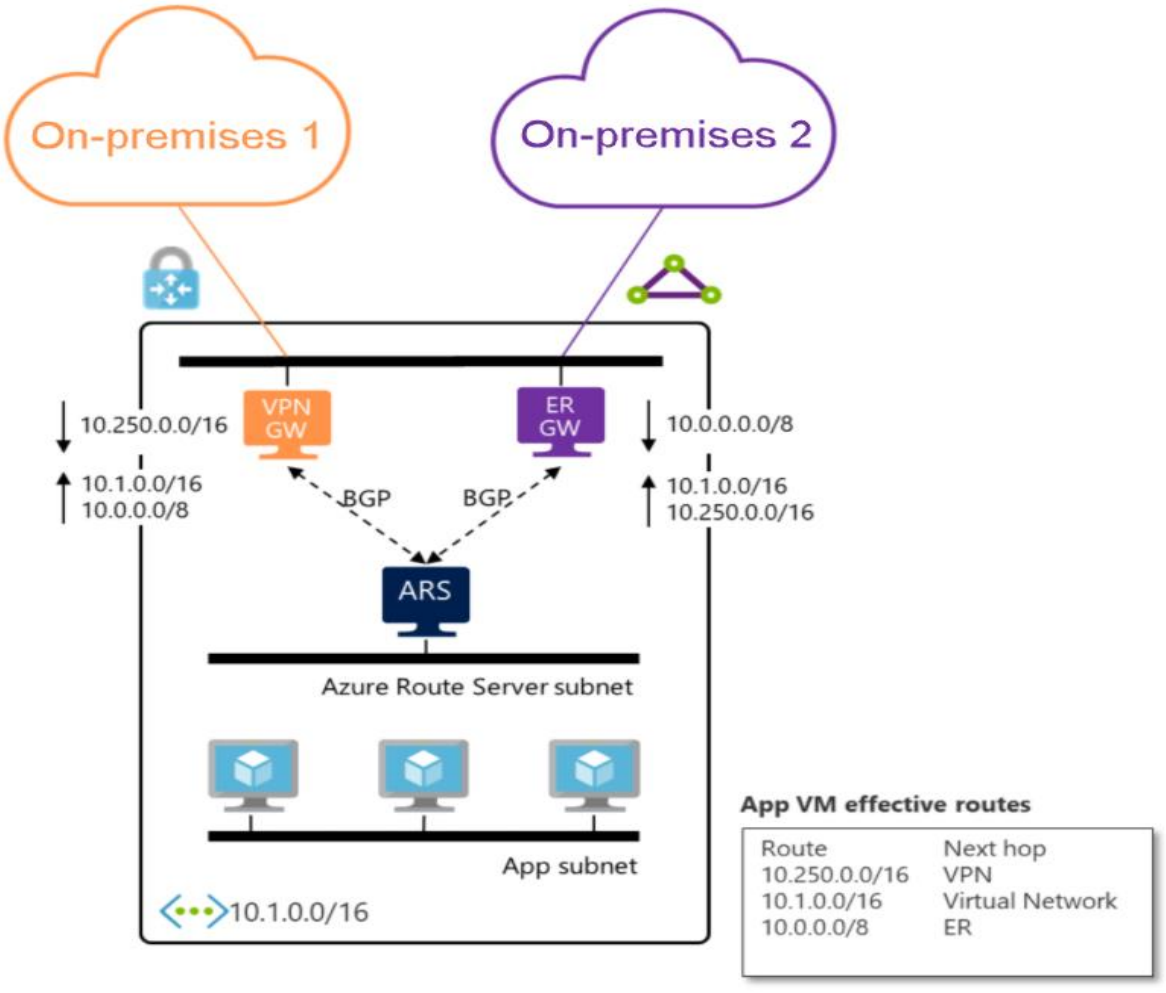
You can use ExpressRoute circuits to establish connectivity across virtual networks within the same geopolitical region or by using the premium add-on for connectivity across geopolitical regions. Keep these points in mind: Network-to-network traffic might experience more latency, because traffic must hairpin at the Microsoft Enterprise Edge (MSEE) routers. The ExpressRoute gateway SKU constrains bandwidth. Deploy and manage UDRs if you need to inspect or log UDRs for traffic across virtual networks. VPN gateways with Border Gateway Protocol (BGP) are transitive within Azure and on-premises networks, but they don't provide transitive access to networks connected via ExpressRoute by default. If you need transitive access to networks connected via ExpressRoute, consider Azure Route Server. When you connect multiple ExpressRoute circuits to the same virtual network, use connection weights and BGP techniques to ensure an optimal path for traffic between on-premises networks and Azure. For more information, see Optimize ExpressRoute routing.



Using BGP metrics to influence ExpressRoute routing is a configuration change made outside of the Azure platform. Your organization or your connectivity provider must configure the on-premises routers accordingly. ExpressRoute circuits with premium add-ons provide global connectivity. ExpressRoute has certain limits; there are a maximum number of ExpressRoute connections per ExpressRoute gateway, and ExpressRoute private peering can identify a maximum number of routes from Azure to on-premises. For more information about ExpressRoute limits, see ExpressRoute limits.

A network architecture deployed within a single Azure region. A network architecture that spans multiple Azure regions, with no need for transitive connectivity between virtual networks for landing zones across regions. A network architecture that spans multiple Azure regions, and global virtual network peering that can connect virtual networks across Azure regions. There's no need for transitive connectivity between VPN and ExpressRoute connections. The main hybrid connectivity method in place is ExpressRoute, and the number of VPN connections is less than 30 per VPN Gateway. There's a dependency on centralized NVAs and granular routing.

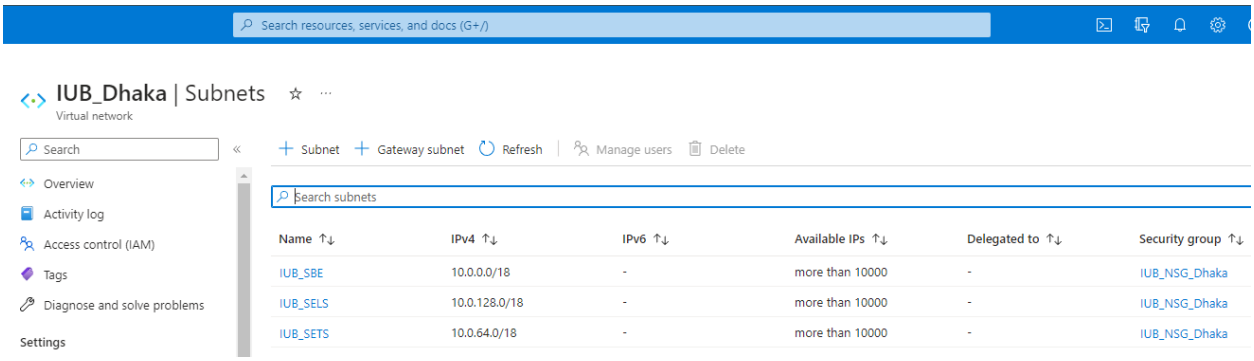
For regional deployments, primarily use the hub-and-spoke topology. Use landing zone virtual networks that connect with virtual network peering to a central hub virtual network for the following scenarios:



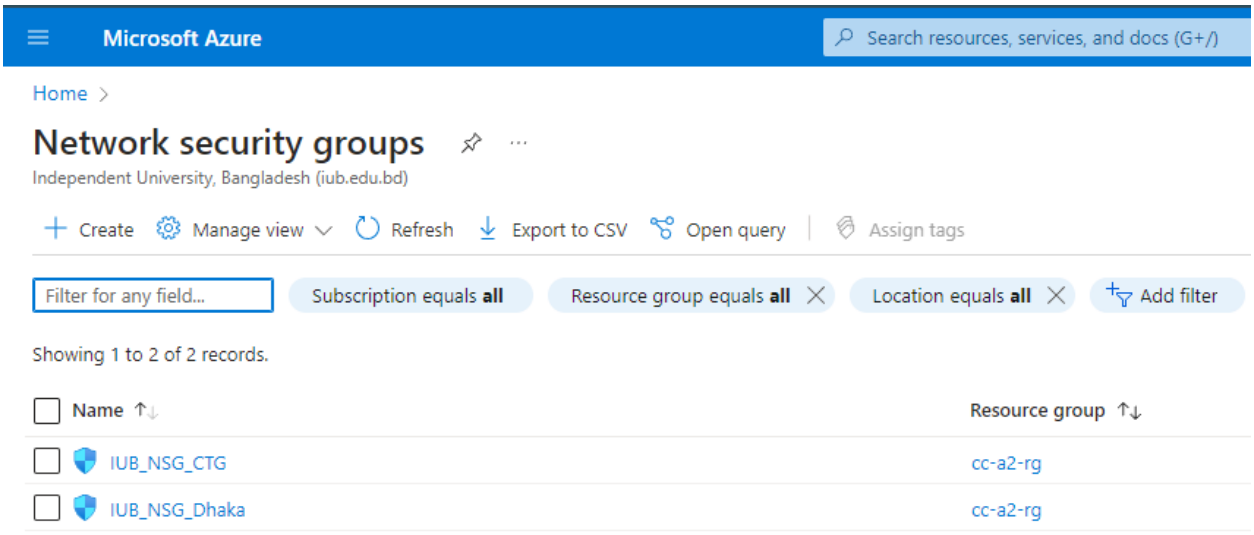
Methodology:

For this project to demonstrate the network topology we have created to Vnets in two different regions such as IUB Dhaka (UK South) and IUB Ctg (UK West) as, establishing connection to a distant location will help us get a much better grasp of the idea.

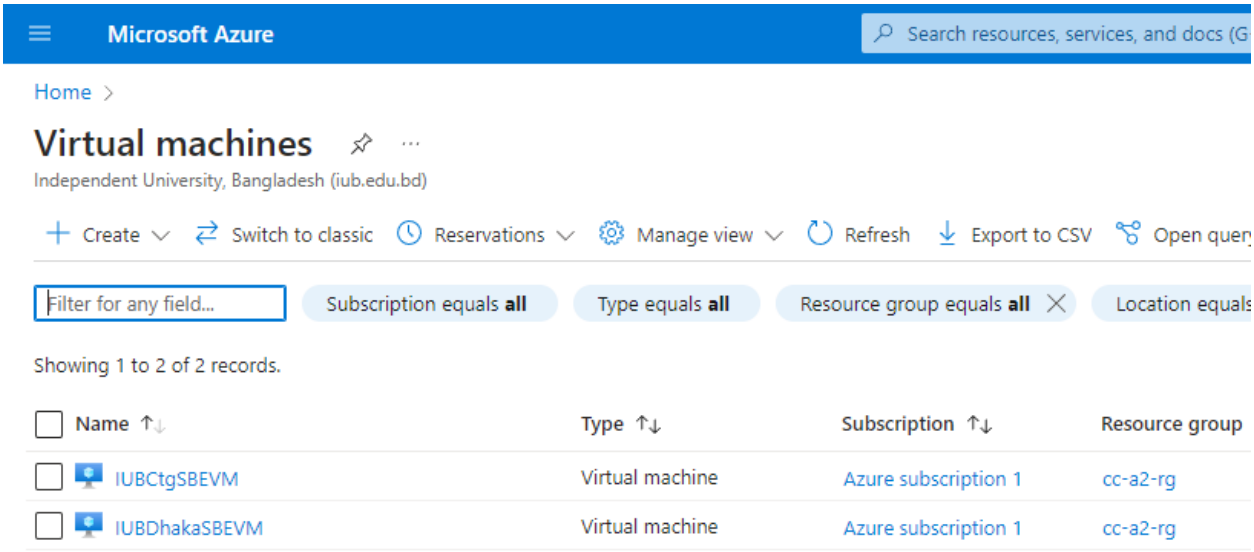
We have created three separate subnets under three different departments such as IUB_SBE, IUB_SETS and IUB_SELS for School of business, School of Engineering and School of Life Sciences on both of the Vnets of Dhaka and Ctg.



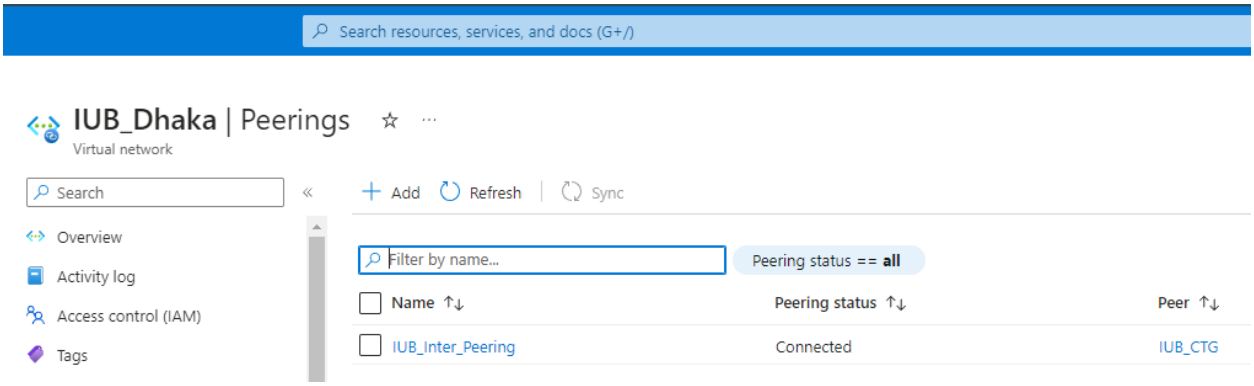
WE have also created the NSG for both of the regional locations with will monitor and maintain network IP and Ports.



Lastly we have created two Virtual Machines on both SBE Dhaka subnet and SBE Ctg subnet which are using the cc-a5-rg resource group, which are using the Standard DS1 v2 (1 vcpu, 3.5 GiB memory) on both VM's and 2016-datacenter-gen2.



We have established Vnet to Vnet peering for communication between two different locations of each departments.



Azure Cost Analysis:

In our project we have chosen to use cheaper and cost effective VM's to save our budget on both regions we have use Microsoft Windows Server 2016 datacenters running on x64 Gen2. Which are the cheapest machines on offer with additional Azure spot discount with Price or capacity so our virtual machine will be evicted when Azure's excess capacity disappears, or costs exceed our specified max price. We decided on selecting the lowest specifications on selection, so we choose the Standard DS1 v2 running on a 1 vcpu and 3.5 GB of memory which gave us $0.01738/hour for our UK south and $0.00883/hour for our UK west VM's selectively. So if we run 3 VM's for each subnets per departments in both Vnets in different locations our monthly bill only on the VM's alone will cost around $19.0728/month for UK west and $37.5408/month for UK south and a total bill of $679.3632/year for IUB but additional costs will also apply if we run a 24x7 continues cloud service such as maintenance and training etc.

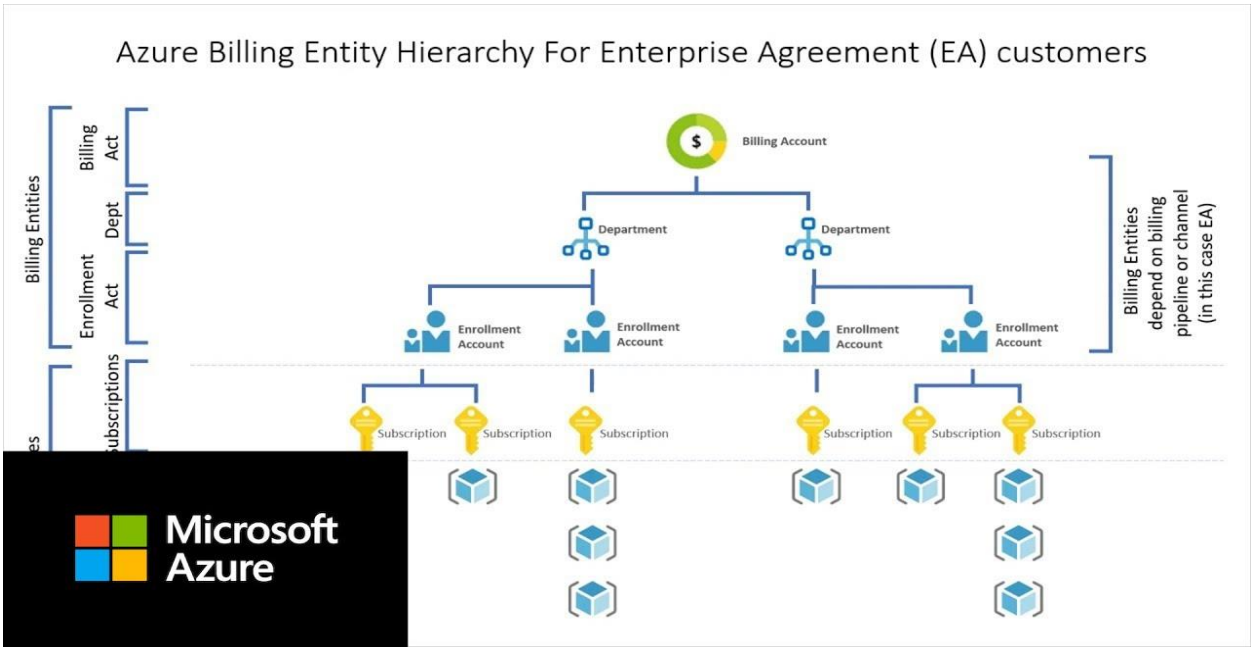
Usage Level % of Billing Cycle	**Incremental Rate** % of On-Demand Baseline	**Sample Rate** n1-standard-1	**Total Cost**
0-25%	100%	$0.050	$9.00
25-50%	80%	$0.040	$7.20
50-75%	60%	$0.030	$5.40
75-100%	40%	$0.020	$3.60
Monthly Cost **at 100% usage**	**30% discount**		**$25.20**

Suggestions and Solutions:

Azure on-premises to cloud migration involves moving an organization's IT infrastructure, applications, and data from their own data centers to the Microsoft Azure cloud. This migration offers numerous benefits, including improved scalability, cost savings, and access to a wide range of cloud services and tools. However, it also requires careful planning, design, and implementation to ensure a successful migration.

The process of migrating from an on-premises network to Azure cloud network involves several stages, including assessing the on-premises environment, selecting Azure services, designing the virtual network, developing a migration plan, deploying Azure services, configuring the virtual network, migrating workloads, testing and validating the migrated environment, and ongoing maintenance and management. When migrating to Azure cloud network, organizations must also consider the potential challenges and drawbacks, such as reliance on Microsoft for network infrastructure and services, possible latency and performance issues, and the need to ensure compliance and security of data stored in the cloud.

Azure cloud migration can offer many benefits for organizations, including improved scalability, cost savings, and access to a wide range of cloud services and tools. However, careful planning and implementation are required to ensure a successful migration and ongoing success of the migrated environment.



Conclusion:

The goal of our project was to simplify the imaginative solutions and explore alternative ideas about broadening our scope for migrate to an easier solution and to improve our digital integrated system for Independent University, Bangladesh.

Overall, we have provided a report that should provide a comprehensive overview of the Azure network migration project, including the planning, implementation, challenges, outcomes, and recommendations for future improvements. It's important to document the process and outcomes of the migration to help identify areas for improvement and ensure ongoing success of the migrated environment.