



CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Manaf Sherjada Khan

College: Lovely Professional University

Department: Cloud Infra & Security

ID: 12207220

Topic 3: - V-Net Peering

1) What is Peering

Peering is a method that allows two networks to connect and exchange traffic directly without having to pay a third party to carry traffic across the Internet.

2) Types of Peering

Peering indicates that two networks connect, but it does not indicate how they are connected. The process could be initiated by running a circuit from one facility to another, but that method becomes inefficient when a network requires multiple peers. Two more common and efficient types of peering are called public peering and private peering.

Public peering

Public peering is generally done through an Internet exchange point (IXP). At these locations, one network can peer with multiple other networks. Peering arrangements need to be negotiated with each peer, but no new cabling needs to be done.

Private peering

Private peering takes place in a colocation facility where two entities with separate networks place routers and run a direct cable between them, rather than using an exchange point switch. This method is useful when networks need to exchange a mass amount of traffic that is unable to fit on a shared connection at an exchange point.

3) What is Network peering?

Network peering works by allowing devices on one network to exchange traffic directly with devices on another network. Peering provides more direct control over how you participate in the internet. For example, a business might have an application hosted on-premises to download data from the public cloud.

4) What is V-Net peering?

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.

Azure supports the following types of peering:

- Virtual network peering: Connecting virtual networks within the same Azure region.
- Global virtual network peering: Connecting virtual networks across Azure regions.

5) What is VM?

A virtual machine (VM) is a virtual environment that functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off- or on-premises). Software called a hypervisor separates the machine's resources from the hardware and provisions them appropriately so they can be used by the VM.

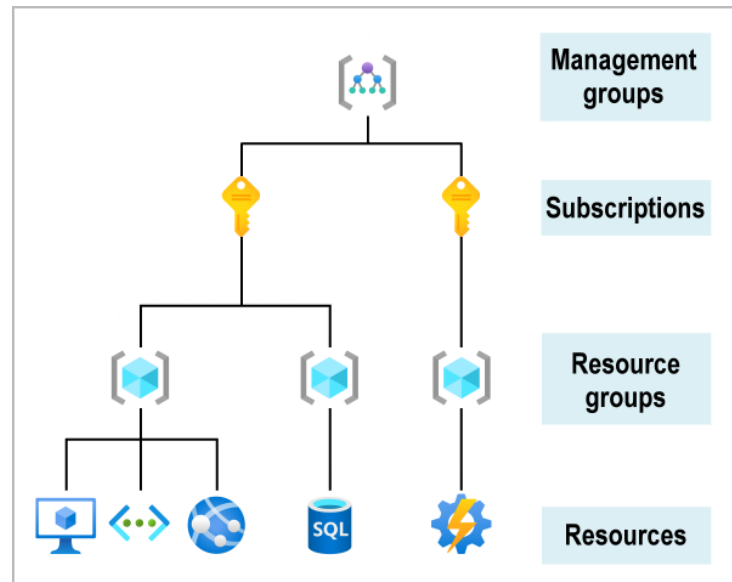
6) What is Inbound and outbound in azure?

Inbound traffic refers to the data coming into your Azure resources from the internet or other networks. In contrast, outbound traffic refers to the data leaving your Azure resources and heading toward other networks.

7) The benefits of using virtual network peering, whether local or global, include:

- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network.
- The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
- The ability to peer virtual networks created through the Azure Resource Manager.
- The ability to peer a virtual network created through Resource Manager to one created through the classic deployment model. To learn more about Azure deployment models, see [Understand Azure deployment models](#).
- No downtime to resources in either virtual network when creating the peering, or after the peering is created.

8) Microsoft Azure hierarchy



Management groups help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions that are applied to the management group.

Subscriptions logically associate user accounts with the resources that they create. Each subscription has limits or quotas on the number of resources that it can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, and projects.

Resource groups are logical containers where you can deploy and manage Azure resources like web apps, databases, and storage accounts.

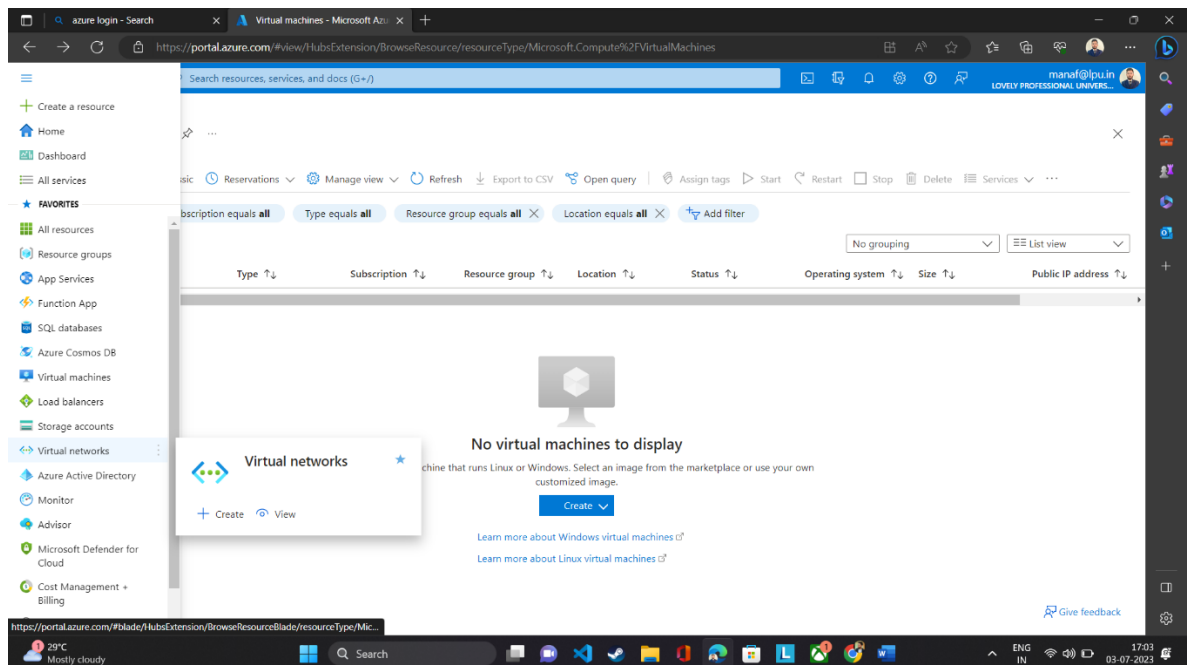
Resources are instances of services that you can create, such as virtual machines, storage, and SQL databases.

9) Practical: - V-net peering?

- Create a virtual Network new (v-net1)
- Create two Virtual machine – v-net1
- RDP
- Window Firewall – off
- CMD – ping private IP

Step 1

First we will create a virtual network



Step 2

Click on create

The screenshot shows the Azure portal interface for 'Virtual networks'. The breadcrumb navigation is 'Home > Virtual networks'. The page title is 'Virtual networks' with a star icon and a close button. Below the title, there are action buttons: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A filter bar shows 'Filter for any field...' and three active filters: 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. A dropdown menu for 'Add filter' is open. The table below shows 'Showing 1 to 1 of 1 records.' with columns for Name, Resource group, Location, and Subscription. The single record is 'vnet1' in resource group 'rg-vet1' located in 'Central India' under the 'Azure for Students' subscription. At the bottom, there are navigation buttons: '< Previous', 'Page 1 of 1', and 'Next >'. The Windows taskbar at the bottom shows the date and time as 17:04 on 03-07-2023.

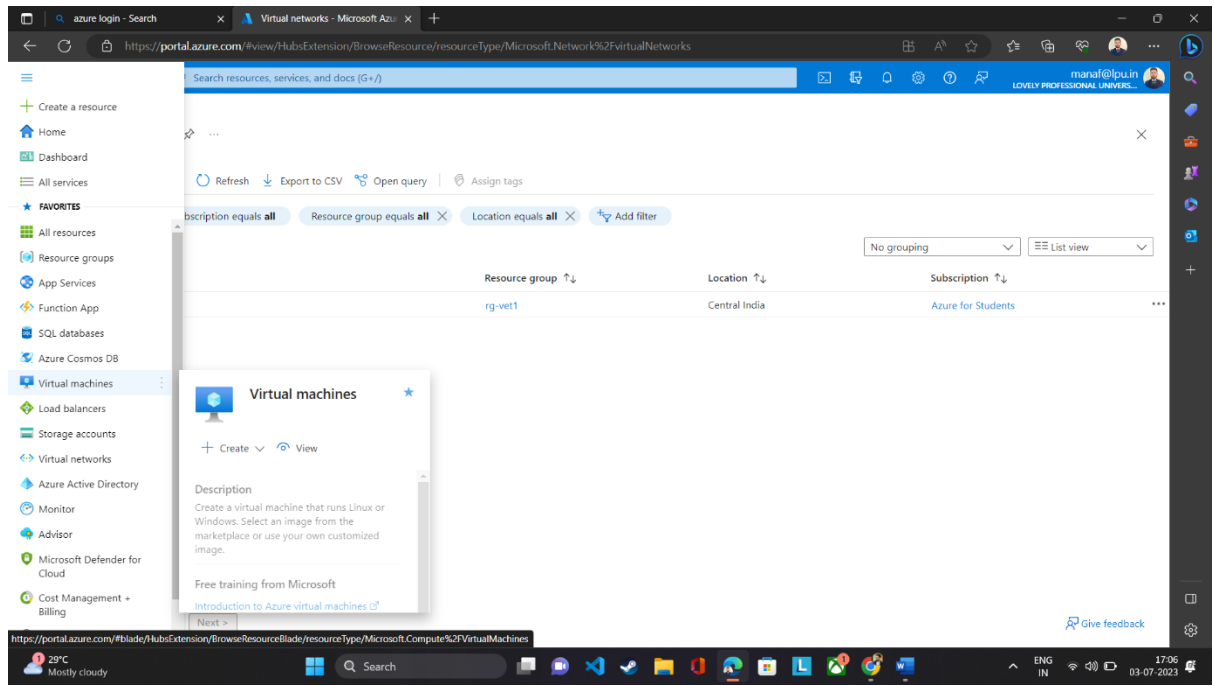
Step 3

Fill the details

The screenshot shows the 'Create virtual network' form in the Azure portal. The breadcrumb navigation is 'Home > Virtual networks > Create virtual network'. The page title is 'Create virtual network' with a close button. Below the title, there are tabs: 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Basics' tab is active. The form contains the following fields: 'Subscription' (Azure for Students), 'Resource group' (rg-vet1), 'Name' (vnet1), and 'Region' (Central India). At the bottom, there are navigation buttons: '< Previous', 'Next: IP Addresses >', and 'Download a template for automation'. The Windows taskbar at the bottom shows the date and time as 17:04 on 03-07-2023.

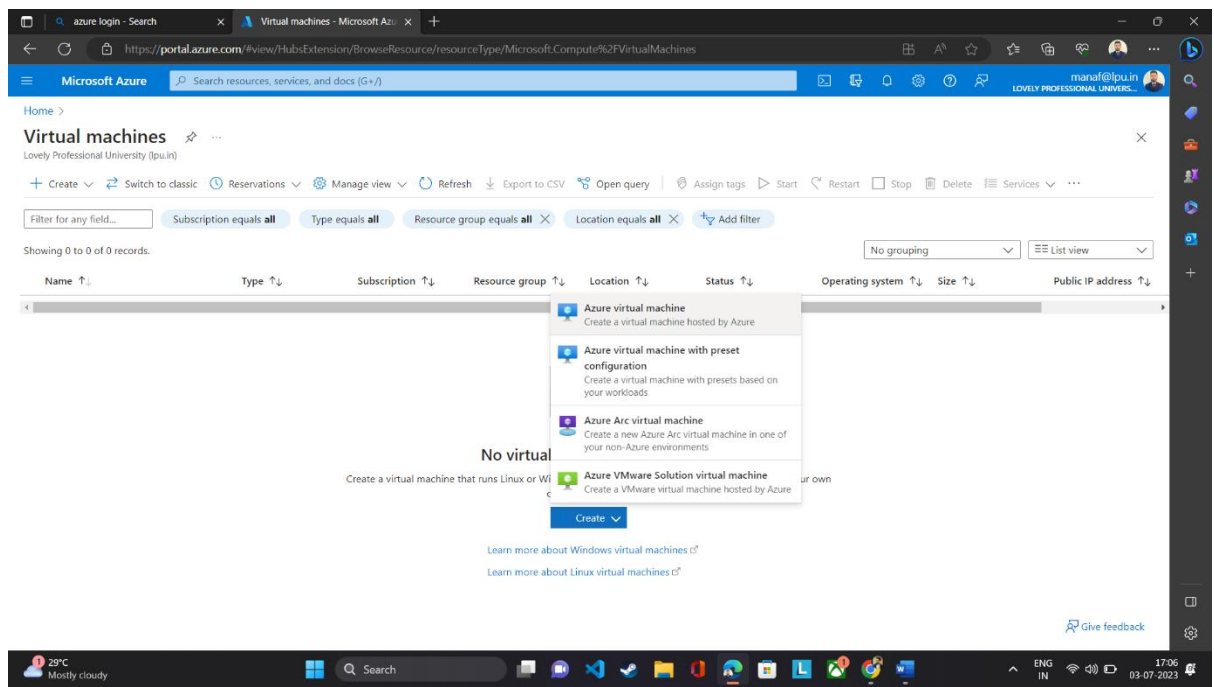
Step 4

Create virtual machine



Step 5

Click on create



Step 6

Fill the details

The screenshot shows the 'Create a virtual machine' page in the Azure portal. The page is titled 'Create a virtual machine' and has a breadcrumb trail 'Home > Virtual machines >'. Below the title, there is a warning message: 'This subscription may not be eligible to deploy VMs of certain sizes in certain regions.' The page is divided into two main sections: 'Project details' and 'Instance details'.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *
[Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Security type
[Configure security features](#)

Image *
[See all images](#) | [Configure VM generation](#)

VM architecture ☐ ☒

At the bottom of the form, there are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Disks >'. On the right side, there is a 'Give feedback' link.

Step 7

In networking part select the same v-net for both the machines

The screenshot shows the 'Create a virtual machine' page in the Azure portal, specifically the 'Networking' tab. The page is titled 'Create a virtual machine' and has a breadcrumb trail 'Home > Virtual machines >'. Below the title, there is a message: 'When creating a virtual machine, a network interface will be created for you.'

Virtual network *
[Create new](#)

Subnet *

Public IP
[Create new](#)

NIC network security group ☐ ☒ ☐

Public inbound ports * ☐ ☒

Select inbound ports *

At the bottom of the form, there is a checkbox labeled 'Delete public IP and NIC when VM is deleted.' which is currently unchecked. Below the checkbox, there are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Management >'. On the right side, there is a 'Give feedback' link.

A warning message is displayed at the bottom of the form: 'This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.'

Step 8

Repeat the same process and Create 2 vms

The screenshot shows the Microsoft Azure portal interface. The main section displays a list of virtual machines under the heading "Virtual machines". The list includes two VMs: "vm1" and "vm2". "vm1" is in the "Running" state, and "vm2" is in the "Creating" state. The table columns are Name, Type, Subscription, Resource group, Location, and Status. A notifications pane on the right shows two successful deployment messages for "CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230703171249" and "CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230703170924" to resource group "rg-vet1".

| Name | Type | Subscription | Resource group | Location | Status |
|------|-----------------|--------------------|----------------|----------------|----------|
| vm1 | Virtual machine | Azure for Students | rg-vet1 | East Asia | Running |
| vm2 | Virtual machine | Azure for Students | RG-VET1 | Southeast Asia | Creating |

Step 9

After creating start both the vm

The screenshot shows the Microsoft Azure portal interface for the "vm1 | Connect" page. The page displays the "Connect with RDP" section, which includes a "Suggested method for connecting" and a "Download RDP File" button. The page also shows the "Overview" tab, "Activity log", "Access control (IAM)", "Tags", and "Diagnose and solve problems" sections.

Connect with RDP

Suggested method for connecting

Azure has checked the status for the most common prerequisites when connecting using this method.

- Checking network security group for inbound access from your client's IP address. [Learn more](#)
- The VM's network interface has a Public IP address. [Learn more](#)
- The VM is running.

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address *
Public IP address (20.24.79.87)

Port number *
3389

[Download RDP File](#)

Can't connect?
[Test network security groups](#)
[Run a comprehensive RDP connectivity test](#)

Step 10

Inside both of the vm check the network

Right click on it and click on ethernet

Go to all about section

And check for the private Ip and remember it

After that from both the vm turn the firewall private and public both so that the data can transfer and it will be in the network > firewall on/off > public off & private off

Then chose any vm and go the cmd (windows command prompt) type the ping (private Ip of the other vm)