IntelliPaat

# Microsoft Azure Administrator Associate Training(AZ-104)

## Module 6

# Agenda

01 Introduction To Microsoft Azure Virtual Network

02 Vnet Components

03 Connecting Different Vnets

04 Vnet Peering

05 Vnet To Vnet Connection Gateway

06 IP Addresses In Azure Vnet

07 IP Address Allocation Method

08 Azure Vnet Routing

09 Azure Network Interface

10 Subnets In Azure VNet

11 Azure DNS

12 Network Security Groups

# Agenda

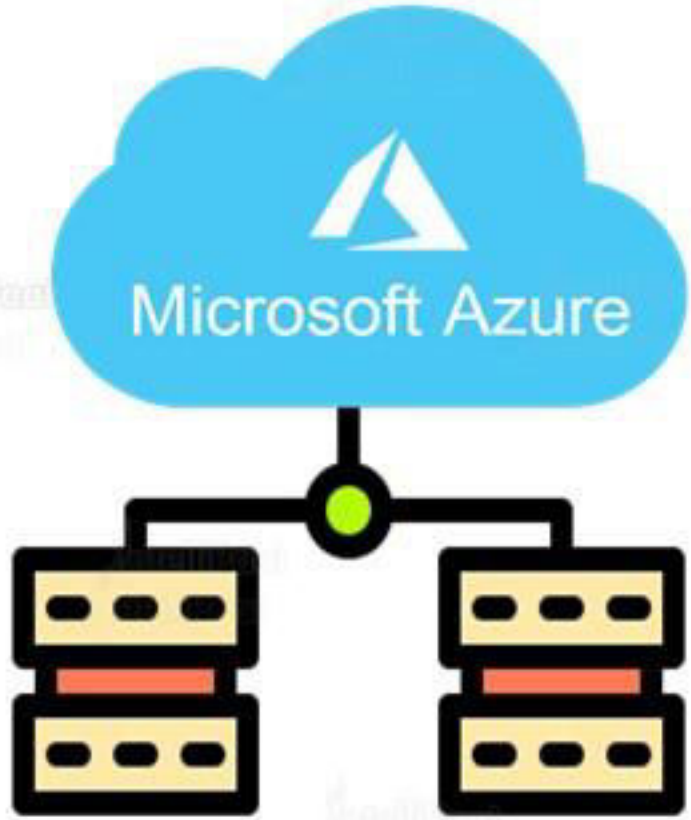
21 Service Tags

23 Quiz

# Introduction to Microsoft Azure Virtual Network

# Introduction to Microsoft Azure Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM) to securely communicate with each other, the Internet, and on-premises networks



# Vnet Components

# VNet Components

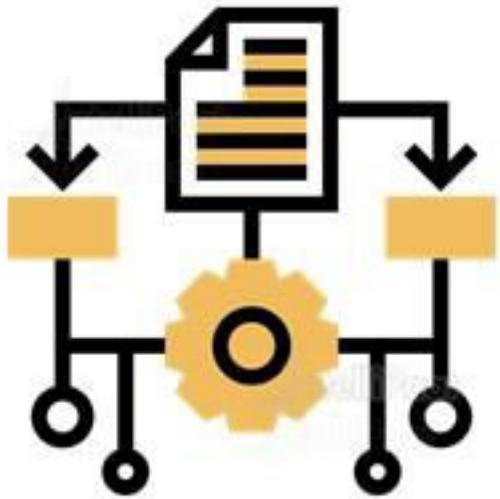
- Address space
- Subnets
- Regions
- Subscription

An Address Space is a range of IP Addresses. Azure will assign the next available IP Address from this address space to a resources in your virtual network.

# VNet Components

- Address space
- Subnets
- Regions
- Subscription

A Subnet is a logical segment of a Virtual Network. A Subnet is allocated a portion of a the virtual network's address space



# VNet Components

- Address space
- Subnets
- Regions
- Subscription

Virtual Networks are scoped to a single location called a region. Multiple virtual networks from different regions can be connected together using Virtual Network Peering

# VNet Components

- Address space
- Subnets
- Regions
- Subscription

Virtual Networks are scoped to a subscription. You can implement multiple virtual networks within each Azure subscription and Azure region.

# Hands-on: Create VNET

# 1. Create a Virtual Network in the Azure Portal

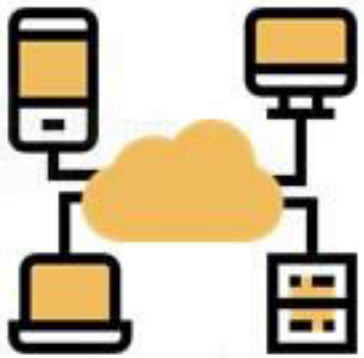
# Connecting Different VNets

# Connecting different VNets

There are two ways you can connect your Azure VNets:

1. VNet Peering

2. VNet to VNet Connection Gateway

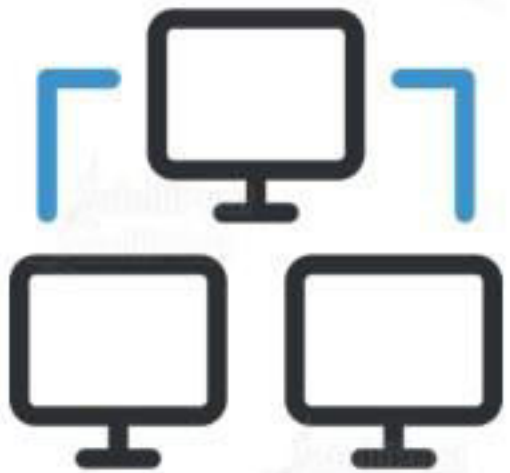


# VNet Peering

# VNet Peering

Virtual network peering enables you to connect to Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes

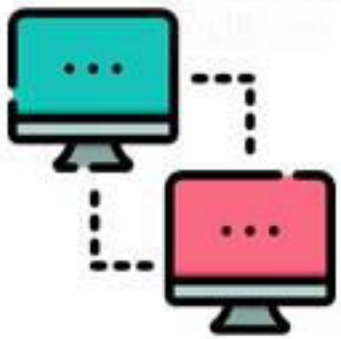
The traffic between virtual machines is routed through the Microsoft infrastructure, through private IP addresses only



# VNet Peering

**Azure supports two types of Virtual Network Peering:**

VNet peering - connecting VNets within the same Azure region



Global VNet peering - connecting VNets across Azure regions

# Hands-on: Create and Configure VNET Peering

# Hands-on

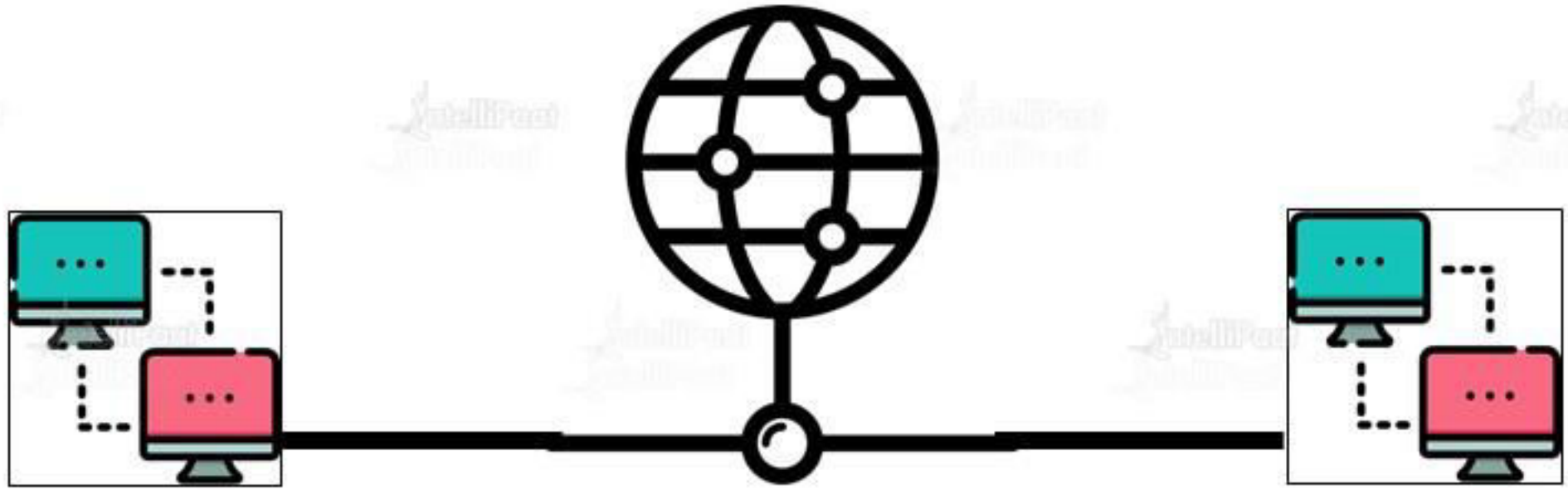
1. Enable Vnet-Vnet Peering between two Virtual Networks

2. Ping one machine's private IP address from another to check if the connection is successful

# VNet to VNet Connection Gateway

# VNet to VNet Connection Gateway

You can connect two VNets to each other using VNet-To-VNet VPN gateway connection. This connection type uses a VPN gateway to provide a secure tunnel with IPsec/IKE and functions the same way when communicating



# IP Addresses

# IP Addresses

You can assign IP addresses to Azure resources to communicate with other Azure resources, your on-premises network, and the Internet.
There are two types of IP addresses you can use in Azure:

1. **Public IP addresses:** Used for communication with the Internet, including Azure public-facing services

2. **Private IP addresses:** Used for communication within an Azure virtual network (VNet) and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

# IP Address Allocation Methods

# IP Address Allocation Methods

There are two methods in which IP addresses are allocated:

**Dynamic**: Azure assigns the next available unassigned or unreserved IP address in the subnet's address range


**Static**: You select and assign any unassigned or unreserved IP address in the subnet's address range

# IP Address Allocation Methods

**Public and Private IP Allocation:**

When a public IP address needs to be assigned to an Azure resource, it is dynamically allocated from a pool of available public IP address within the location the resource is created

A private IP address can be allocated with either Dynamic Allocation or Static Allocation

# Hands-on: Assign Static IP to VM

# Hands-on

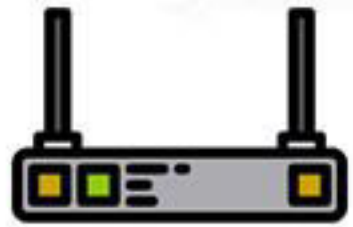
1. Deploy a Virtual Machine

2. Go to IP Configurations and Apply a static IP address to the machine

# Azure VNet Routing

# Azure VNet Routing

Routing traffic between different subnets in a virtual network is taken care of by Azure



You can create your own routes to override Azure's default routing

# Hands-on: Create a Route Table

# Hands-on: Add Route to Route Table

# Hands-on

1. Deploy a Routing table

2. Add routes to the table

3. Verify the routes by checking if the IP address has been redirected successfully

# Azure Network Interface

# Azure Network Interface

A network interface (NIC) is the interconnection between a Virtual Machine and a virtual network

A VM must have at least one NIC, but can have more than one

Multiple Network Interfaces allow a VM to connect to different subnets and send or receive traffic over the most appropriate interface

# Hands-On: Create NIC

# Hands-on: Attach NIC to VM

# Hands-on

1. Create a NIC for a subnet

2. Attach the NIC to a Virtual Machine and verify the access changes

# Azure Subnets

# Why Subnets?

# Azure Subnets

A subnet is a partition of your virtual network in Azure VNet

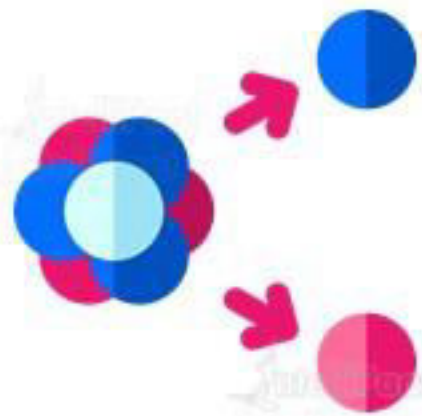
Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address

Subnets were initially designed for solving the shortage of IP addresses over the Internet

# Why Subnets?

- Logical divisions
- Improved network security
- Improved network performance

Subnetting helps you maintain clean separations within a network. This separation helps in maintaining a large network



# Why Subnets?

IntelliPaat

**Logical divisions**

**Improved network security**

**Improved network performance**

With logical divisions between subnets, you have greater control over who has access to what

# Why Subnets?

- Logical divisions
- Improved network security
- Improved network performance

Subnetting reduces the amount of broadcast traffic by containing network broadcasts at the subnet level instead of sending all broadcasts to the entire network

# Azure DNS

# Azure DNS

Azure DNS is a hosting service for DNS domains that provide name resolution by using Microsoft Azure infrastructure.

The Domain Name System, or DNS, is responsible for converting a URI to its IP address

# Why Azure DNS?

- Reliability and performance
- Security
- Ease of use
- Alias records

In Azure DNS, each DNS query is responded to by the closest available DNS server

# Why Azure DNS?

- Reliability and performance
- Security
- Ease of use
- Alias records

Azure DNS is based on Azure Resource Manager (ARM), which provides various security features such as Role-based access control, Activity logs, and Resource locking

# Why Azure DNS?

- Reliability and performance
- Security
- Ease of use
- Alias records

Azure DNS can manage DNS records for your Azure services and provide DNS for your external resources as well

# Why Azure DNS?

- Reliability and performance
- Security
- Ease of use
- Alias records

Alias Records are used to refer to an Azure resource, such as an Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network (CDN) endpoint

# Hands-on: Create DNS Zone

# Hands-on: Add Record Set to DNS Zone

# Hands-on

1. Create a DNS Zone in the Azure Portal

2. Change the name server address in your domain name provider website and create a Record Set

3. Verify the website is running on the domain

# Azure Private DNS

Azure Private DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network

Private DNS allows you to use your own custom domain names rather than the Azure-provided ones


It provides name resolution for virtual machines (VMs) within a virtual network and between virtual networks

# Network Security Groups

# Azure Security Group

A network security group is used to encapsulate rules to filter incoming and outgoing traffic to and from several types of Azure resources

For each rule, you can specify source and destination, port, and protocol

# Security Rules

# Azure Security Rules

A Security Rule is used in Azure to specify some constraint on incoming or outgoing traffic.

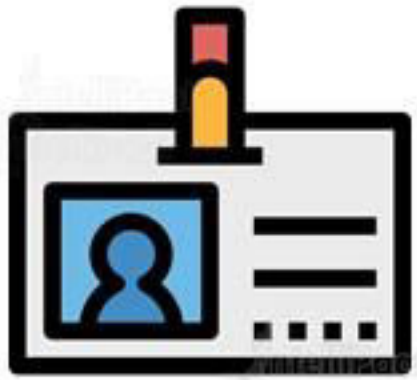
Each rule specifies some properties

# Security Rule Properties

# Security Rule Properties

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

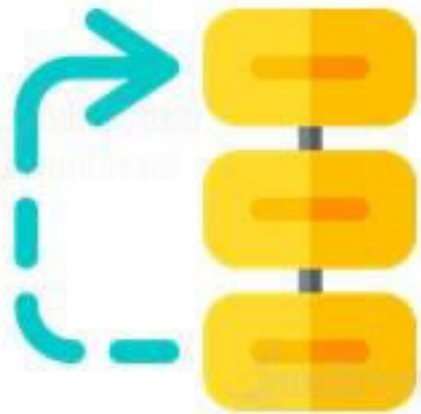
It is a unique name within the network security group which is used to identify and refer to a rule



# Security Rule Properties

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

It indicates a number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers. Once traffic matches a rule, processing stops



# Security Rule Properties

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

Any, or an individual IP address

# Security Rule Properties

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

TCP, UDP, ICMP, or others

# Security Rule Properties

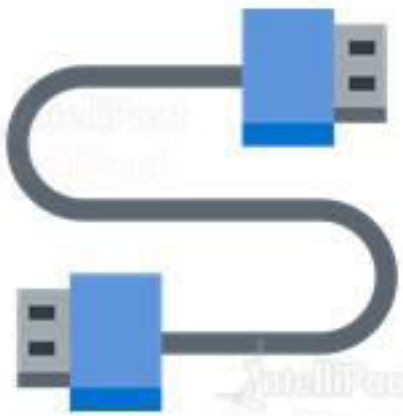
- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

It indicates whether the rule applies to inbound or outbound traffic

# Security Rule Properties

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

You can specify an individual or range of ports for your rules. Specifying ranges enables you to create fewer security rules



# Security Rule Properties

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

Action indicates whether to allow or deny traffic

# Hands-on: Create NSG

# Hands-on: Attach NSG to a Subnet

# Hands-on: Verify NSG is Applied

# Hands-on

1. Create an NSG in the Azure portal

2. Associate this NSG with a subnet where the changes must be applied

3. Verify the connections in the NSG by verifying the resources deployed in that subnet (Virtual Machine)

# Service Tags

# Service Tags

A service tag is used to group IP Addresses to make it easy to apply security rules.

Service tags allow easy creation and allow to minimize complexity of rule creation.

Service Tags are managed by Azure. You cannot create or assign your own service tags.

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24/7 Chat with Our Course Advisor