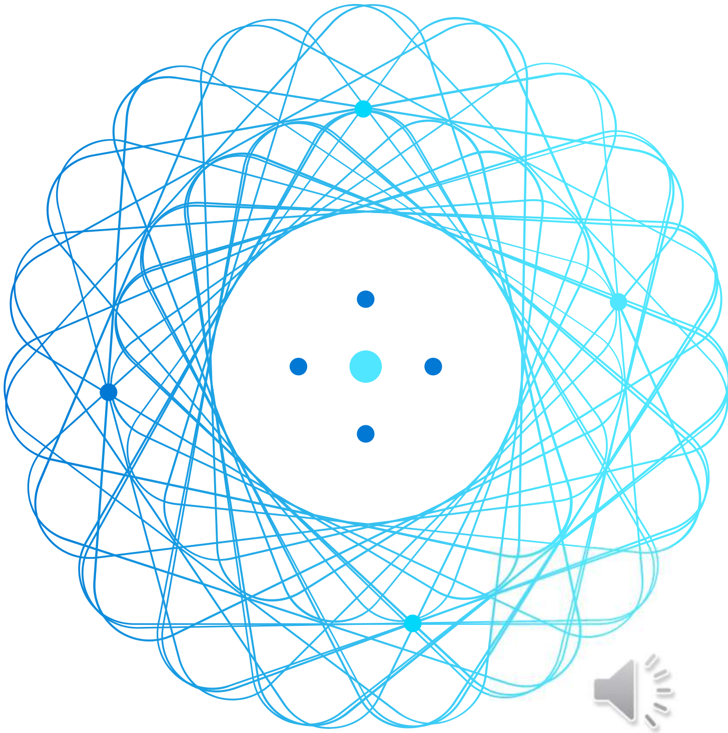
Microsoft Azure

Azure Networking



Compute and Networking- Objective Domain

Describe the benefits and usage of:

- Virtual Networks
- Azure Virtual Networks
- Azure virtual subnets
- VNET peering
- Azure DNS
- VPN Gateway
- ExpressRoute
- Public and private endpoints.

https://docs.microsoft.com/learn/modules/describe-azure-compute-networking-services/1-introduction

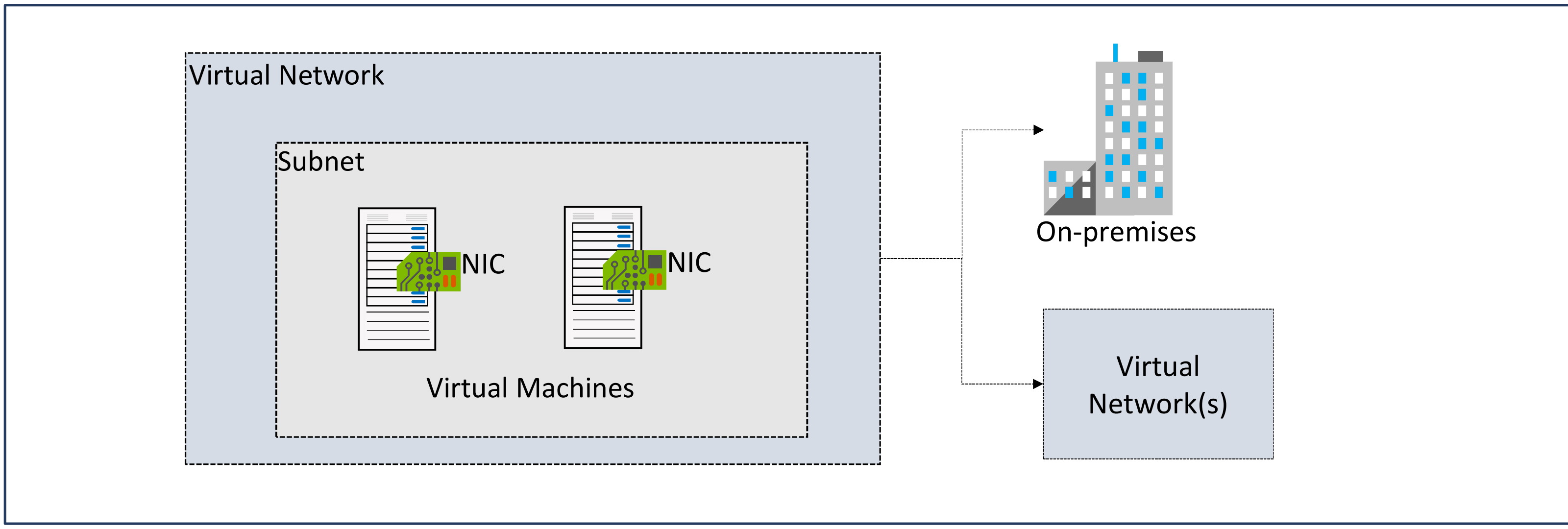
Azure networking services

Azure Virtual Network (VNet) enables Azure resources to communicate with each other, the internet, and on-premises networks.

- Public endpoints, accessible from anywhere on the internet
- Private endpoints, accessible only from within your network
- Virtual subnets, segment your network to suit your needs
- Network peering, connect your private networks directly together

https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/8-virtual-network

Virtual Networks – Planning & Designing



Logical representation of your own network

Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

Enable hybrid cloud scenarios

Azure Virtual Networks - https://azure.microsoft.com/services/virtual-network/

What is Azure Virtual Network? - https://docs.microsoft.com/azure/virtual-network/virtual-networks-overview

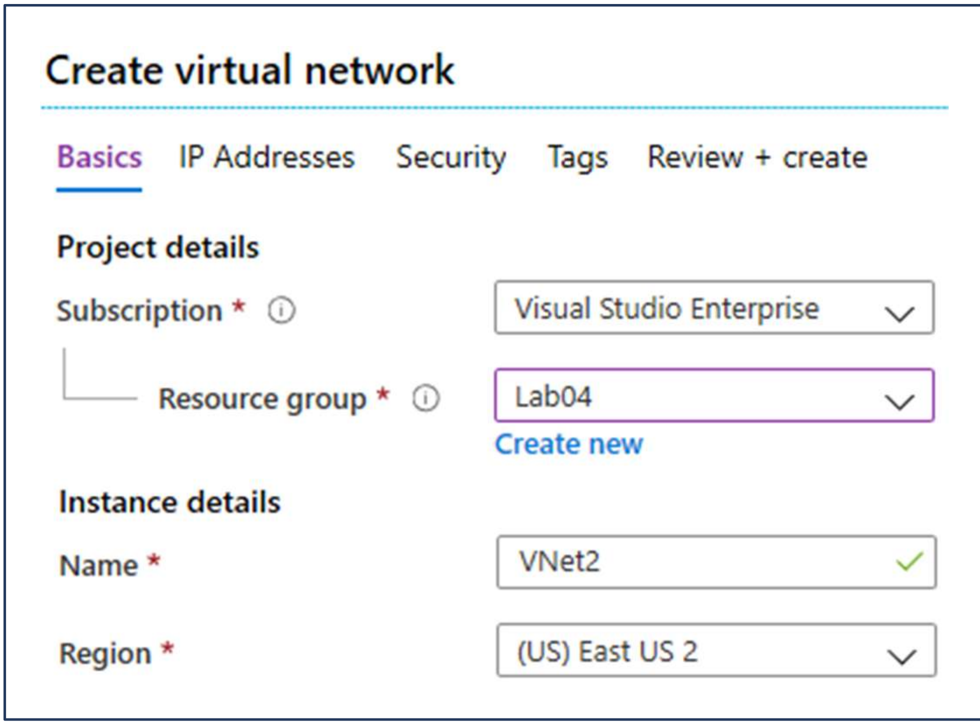
Create Virtual Networks

Create new virtual networks at any time

Add virtual networks when you create a virtual machine

Need to define the address space, and at least one subnet

Be careful with overlapping address spaces



Create virtual network

Project details

Subscription * Visual Studio Enterprise

Resource group * Lab04

Instance details

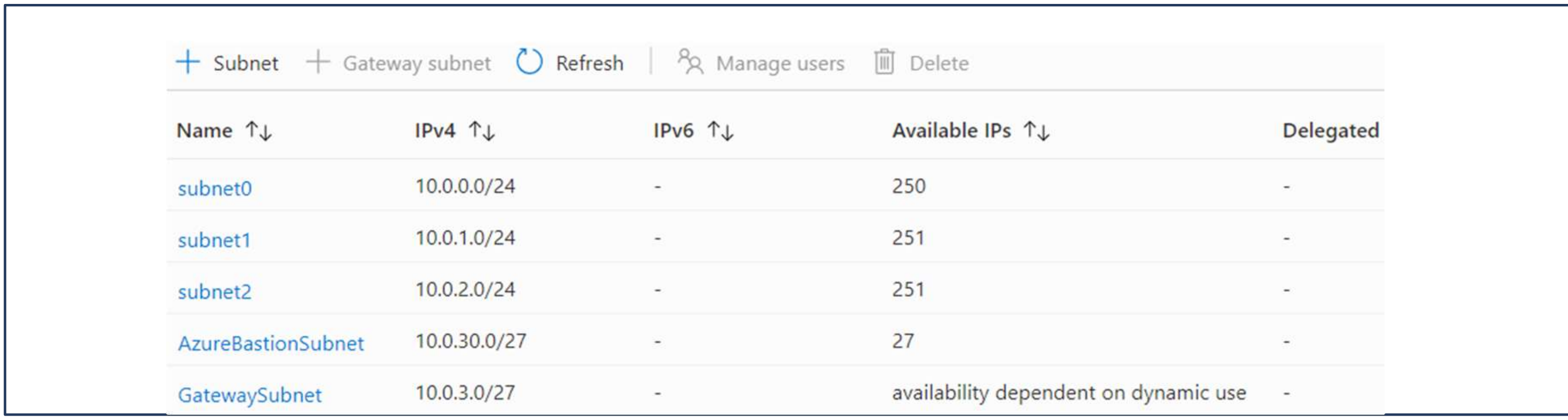
Name * VNet2

Region * (US) East US 2

QuickStart: Create a virtual network using the Azure portal - https://docs.microsoft.com/azure/virtual-network/quick-create-por

✓ Always plan to use an address space that is not already in use in your organization, either on-premises or in other VNets. Eve if you plan for a VNet to be cloud-only, you may want to make a VPN connection to it later. If there is any overlap in address spac at that point, you will have to reconfigure or recreate the VNet. The next lesson will focus on IP addressing.

Create Subnets



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/27	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

A virtual network can be segmented into one or more subnets

Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

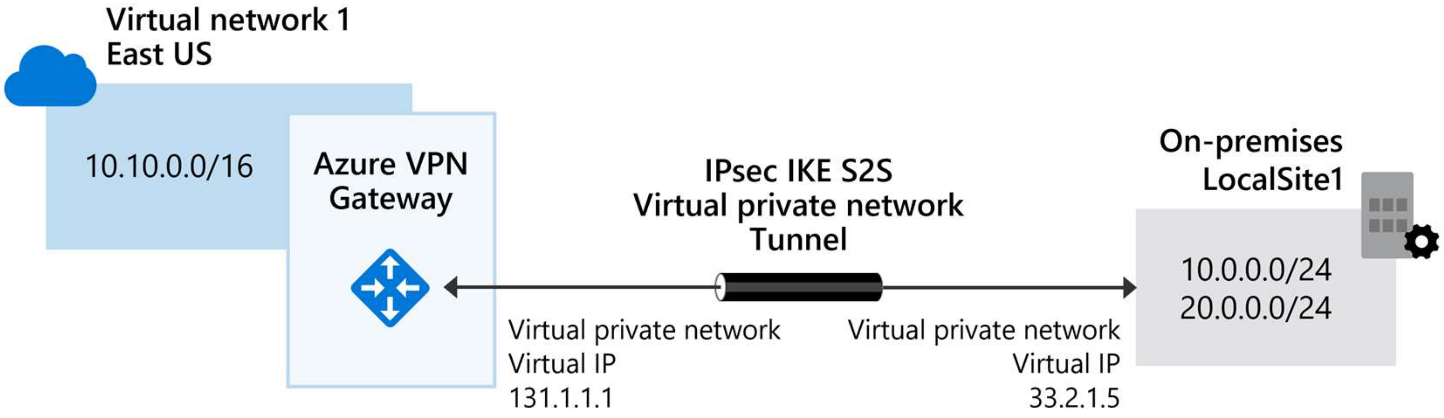
Each subnet must have a unique address range – cannot overlap with other subnets in the vnet in the subscription

✓ Azure reserves 5 IP addresses within each subnet.

- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address

Azure networking services

Virtual Private Network Gateway (VPN) is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet.



https://docs.microsoft.com/learn/modules/describe-azure-compute-networking-services/10-virtual-private-networks

Azure VPN Gateway is a service that uses a specific type of virtual network gateway to send encrypted traffic between Azure virtual network and on-premises locations over the public Internet, or between two Azure Virtual Networks.

After you create a VPN gateway, you can configure connections.

- For example, you can create an [IPsec/IKE] VPN tunnel connection between that VPN gateway and another VPN gateway (VNet-to-VNet), or
- Create a cross-premises [IPsec/IKE] VPN tunnel connection between the VPN gateway and an on-premises VPN device (Site-to-Site).

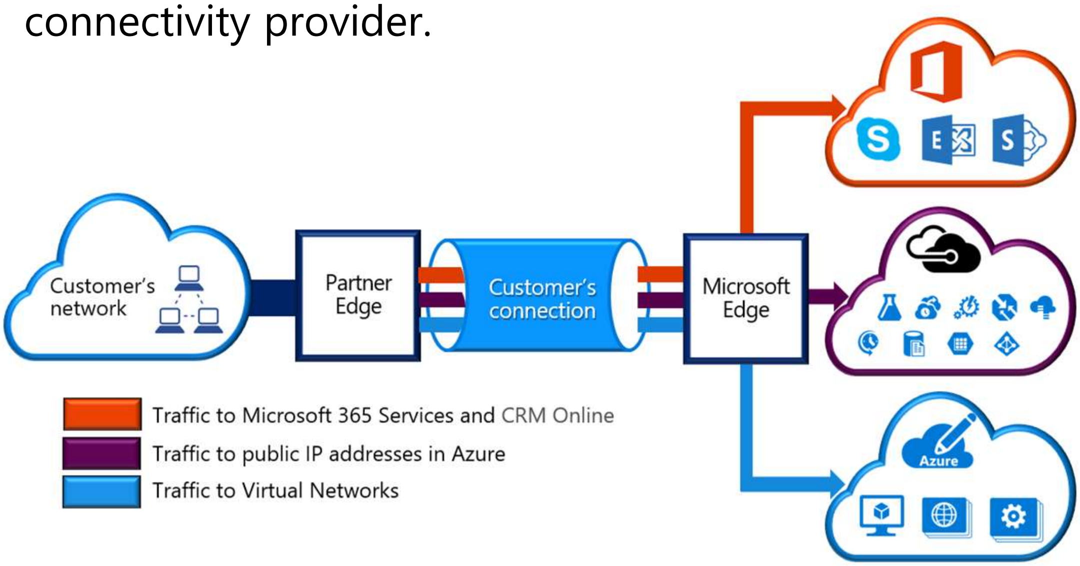
Optional

IPSEC/IKE v1

[Understand IPsec IKEv1 Protocol - Cisco]

Azure networking services

Azure Express Route extends on-premises networks into Azure over a private connection that is facilitated by a connectivity provider.


Customer's network
Partner Edge
Customer's connection
Microsoft Edge
Azure
🟧 Traffic to Microsoft 365 Services and CRM Online
🟪 Traffic to public IP addresses in Azure
🟦 Traffic to Virtual Networks

https://docs.microsoft.com/learn/modules/describe-azure-compute-networking-services/11-expressroute/

ExpressRoute – Features and Benefits

ExpressRoute enables direct access to the following services in all regions:

- Microsoft Office 365
- Microsoft Dynamics 365
- Azure compute services, such as Azure Virtual Machines
- Azure cloud services, such as Azure Cosmos DB and Azure Storage

ExpressRoute – Global Reach

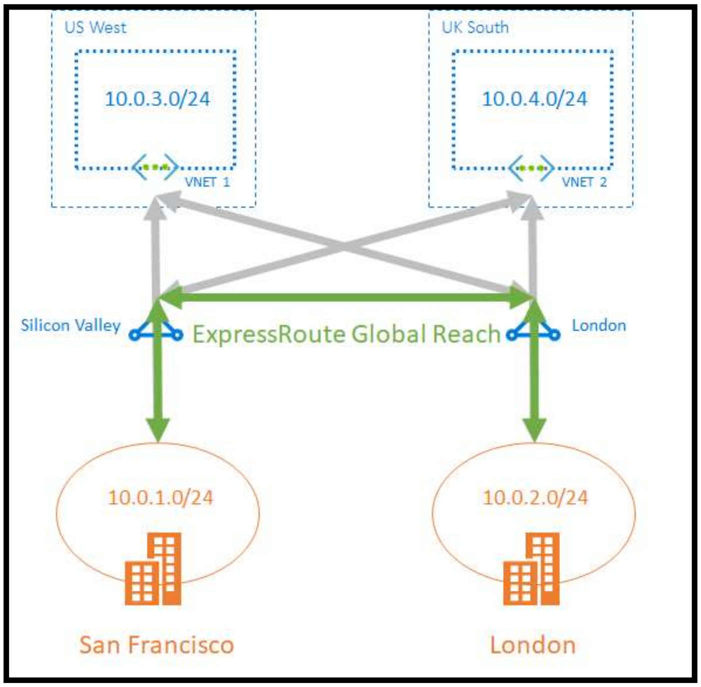
You can enable ExpressRoute Global Reach to exchange data across your on-premises sites through Microsoft Network by connecting your ExpressRoute circuits.

For example, assume you have an office in Asia and a datacenter in Europe, both with ExpressRoute circuits connecting them to the Microsoft network.

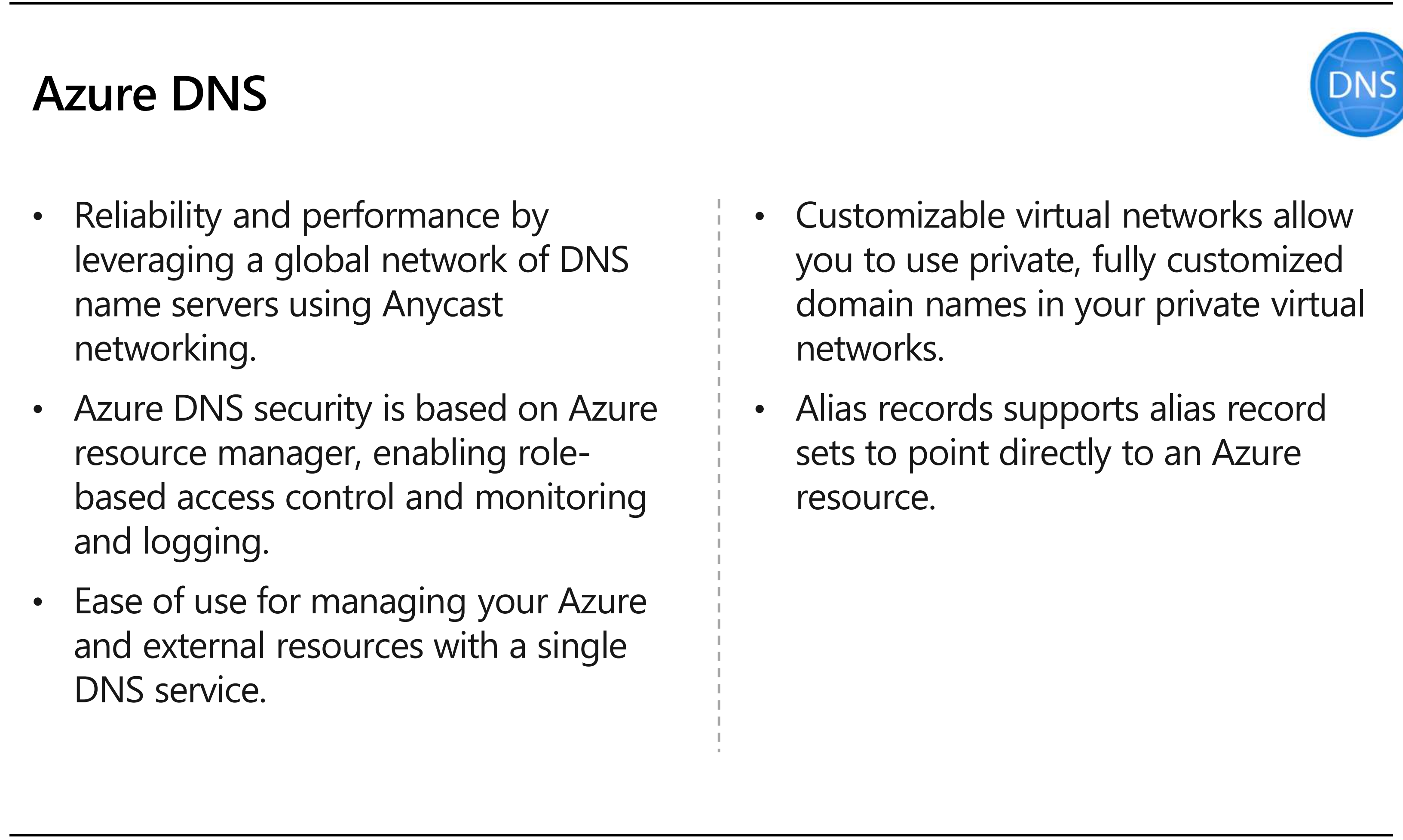
You could use ExpressRoute Global Reach to connect those two facilities, allowing them to communicate without transferring data over the public internet.

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks.

In our example to the right, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.



https://learn.microsoft.com/en-us/azure/expressroute/expressroute-global-reach



Azure DNS

- Reliability and performance by leveraging a global network of DNS name servers using Anycast networking.
- Azure DNS security is based on Azure resource manager, enabling role-based access control and monitoring and logging.
- Ease of use for managing your Azure and external resources with a single DNS service.
- Customizable virtual networks allow you to use private, fully customized domain names in your private virtual networks.
- Alias records supports alias record sets to point directly to an Azure resource.

https://docs.microsoft.com/learn/modules/describe-azure-compute-networking-services/12-domain-name-system

Anycast:
[Anycast DNS overview | Microsoft Learn]
[What is Anycast DNS? | How Anycast works with DNS | Cloudflare]

Azure Private DNS

- Azure Private DNS provides a reliable and secure DNS service for your virtual networks.
- Azure Private DNS manages and resolves domain names in the virtual network without the need to configure a custom DNS solution.
- To resolve the records of a private DNS zone from your virtual network, you must link the virtual network with the zone.
- Linked virtual networks have full access and can resolve all DNS records published in the private zone.
- You can also enable autoregistration on a virtual network link.
- When you enable autoregistration on a virtual network link, the DNS records for the virtual machines in that virtual network are registered in the private zone.
- When autoregistration gets enabled, Azure DNS will update the zone record whenever a virtual machine gets created, changes its' IP address, or gets deleted.

What is Azure Private DNS? | Microsoft Learn

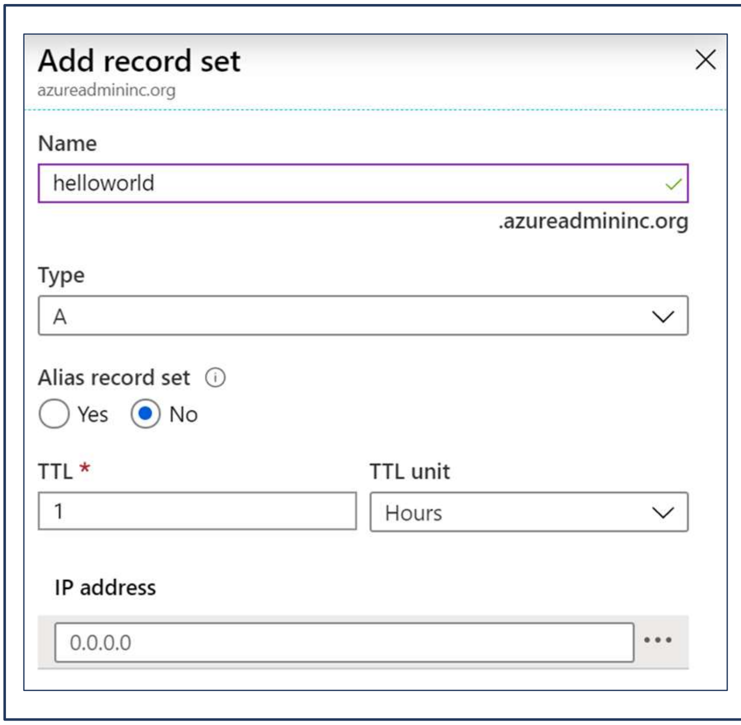
Add DNS Record Sets

A record set is a collection of records in a zone that have the same name and are the same type

You can add up to 20 records to any record set

A record set cannot contain two identical records

Changing the drop-down Type, changes the information required



Add record set
azureadmininc.org

Name
helloworld
.azureadmininc.org

Type
A

Alias record set
○ Yes ● No

TTL *
1

TTL unit
Hours

IP address
0.0.0.0

Plan for Private DNS Zones

Use your own custom domain names

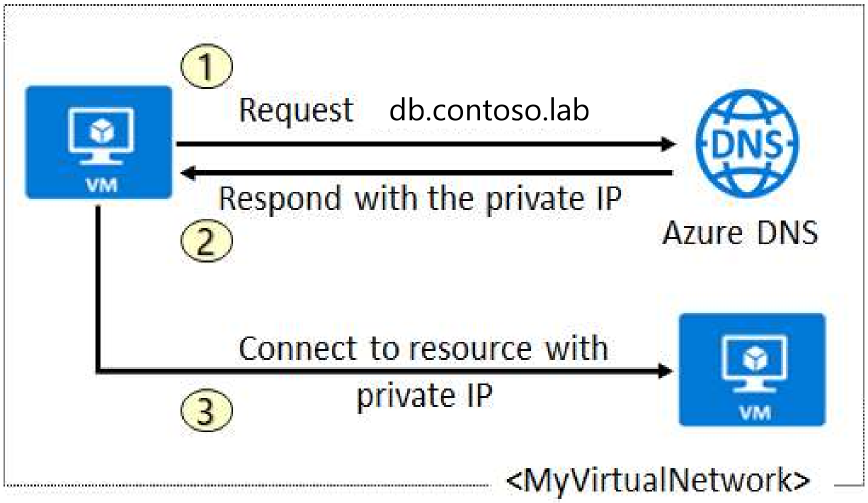
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

Removes the need for custom DNS solutions

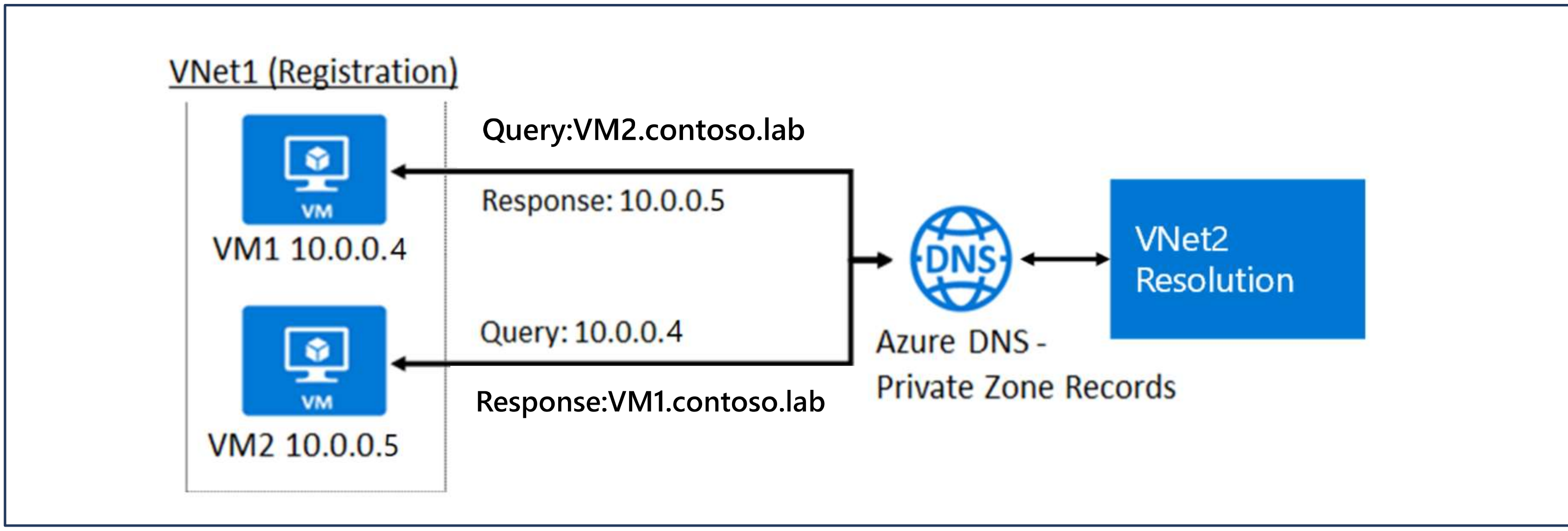
Use all common DNS records types

Available in all Azure regions


1
Request db.contoso.lab
VM
DNS
Respond with the private IP
2
Azure DNS
Connect to resource with private IP
3
VM
<MyVirtualNetwork>

QuickStart: Create an Azure private DNS zone using the Azure portal - https://docs.microsoft.com/azure/dns/private-dns-getstarted-portal

Determine Private Zone Scenarios



DNS resolution in VNet1 is private and not accessible from the Internet

DNS queries across the virtual networks are resolved

Reverse DNS queries are scoped to the same virtual network

Azure Traffic Manager

- Azure Traffic Manager is a DNS-based traffic load balancer.
- This service allows you to distribute traffic to your public facing applications across the global Azure regions.
- Traffic Manager also provides your public endpoints with high availability and quick responsiveness.
- Traffic Manager uses DNS to direct client requests to the appropriate service endpoint based on a traffic-routing method.
- Traffic manager also provides health monitoring for every endpoint.

Azure Traffic Manager | Microsoft Learn

Traffic Manager – Routing Methods

- **Priority**: Select **Priority** routing when you want to have a primary service endpoint for all traffic. You can provide multiple backup endpoints in case the primary or one of the backup endpoints is unavailable.
- **Weighted**: Select **Weighted** routing when you want to distribute traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.
- **Performance**: Select **Performance** routing when you have endpoints in different geographic locations, and you want end users to use the "closest" endpoint for the lowest network latency.

Azure Traffic Manager - traffic routing methods | Microsoft Learn

Traffic Manager – Routing Methods (cont…)

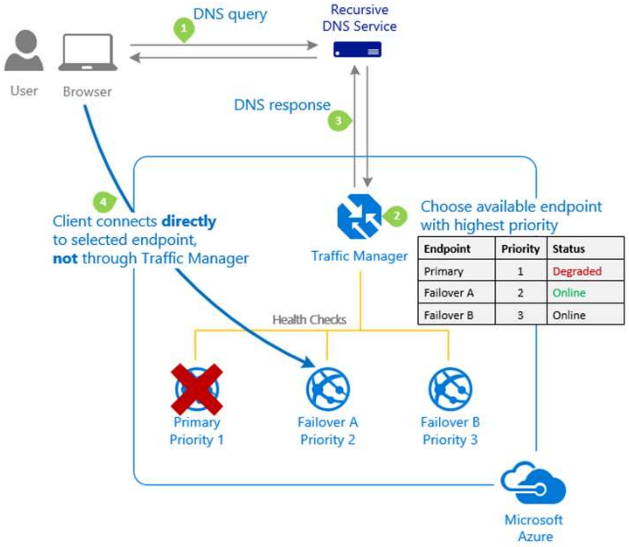
•**Geographic:** Select **Geographic** routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.

•**Multivalue:** Select **MultiValue** for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.

•**Subnet:** Select **Subnet** traffic-routing method to map sets of end-user IP address ranges to a specific endpoint. When a request is received, the endpoint returned will be the one mapped for that request's source IP address.

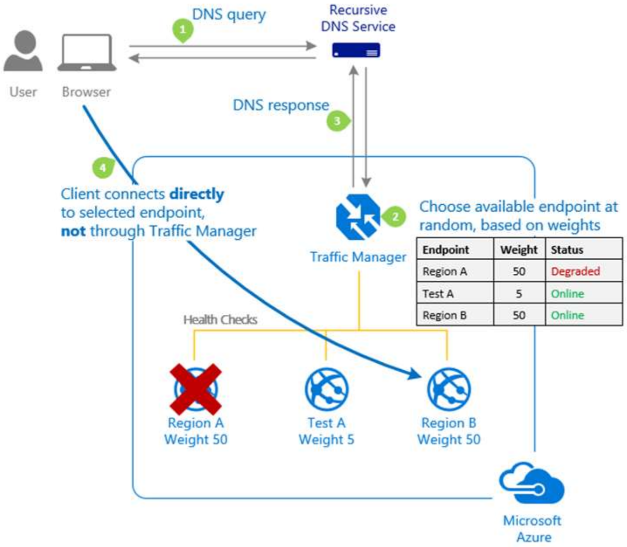
Azure Traffic Manager - traffic routing methods | Microsoft Learn

Priority traffic-routing



Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

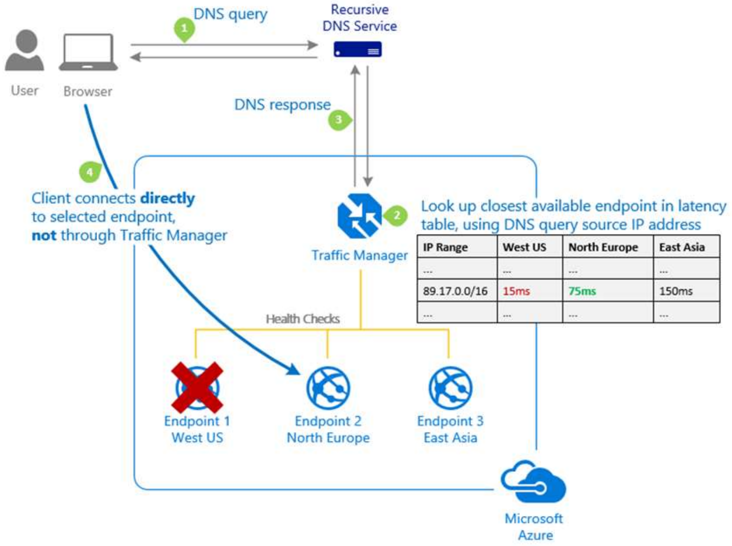
| Weighted traffic-routing



Endpoint	Weight	Status
Region A	50	Degraded
Test A	5	Online
Region B	50	Online

Azure Traffic Manager - traffic routing methods | Microsoft Learn

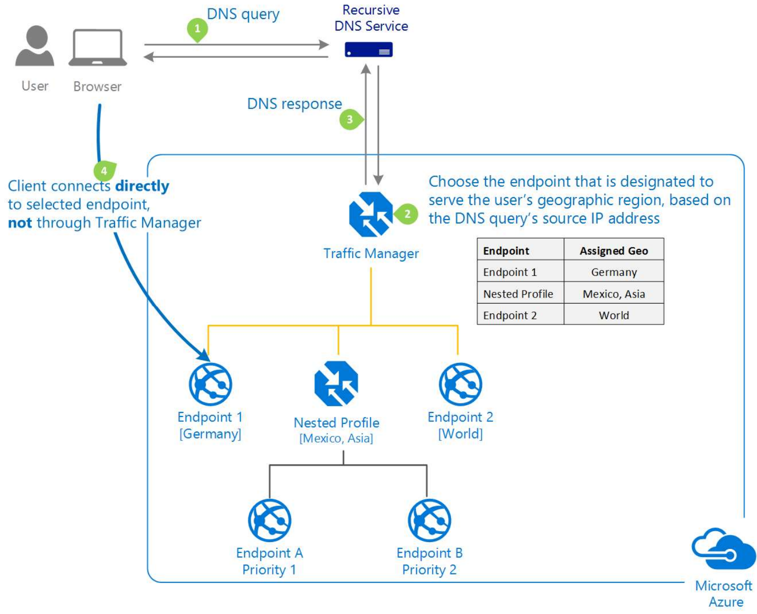
Performance traffic-routing | Geographic traffic-routing



Client connects **directly** to selected endpoint, **not** through Traffic Manager

Look up closest available endpoint in latency table, using DNS query source IP address

IP Range	West US	North Europe	East Asia
...	...	...	...
89.17.0.0/16	15ms	75ms	150ms
...	...	...	...



Client connects **directly** to selected endpoint, **not** through Traffic Manager

Choose the endpoint that is designated to serve the user's geographic region, based on the DNS query's source IP address

Endpoint	Assigned Geo
Endpoint 1	Germany
Nested Profile	Mexico, Asia
Endpoint 2	World

[Azure Traffic Manager - traffic routing methods | Microsoft Learn]

Multivalue traffic-routing | Subnet traffic-routing

- The **Multivalue** traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response.
- This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive.
- This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint.

- The **Subnet** traffic-routing method allows you to map a set of end-user IP address ranges to specific endpoints in a profile.
- If Traffic Manager receives a DNS query for that profile, it will inspect the source IP address of that request.
- It will then determine which endpoint it's mapped to and will return that endpoint in the query response.

Azure Traffic Manager - traffic routing methods | Microsoft Learn

Subnet Traffic-Routing Method

- Subnet routing can be used to deliver a different experience for users connecting from a specific IP space.
- For example, you can make all requests from your corporate office be routed to a different endpoint.
- This routing method is especially useful if you're trying to test an internal only version of your app.
- Another scenario is if you want to provide a different experience to users connecting from a specific ISP (For example, block users from a given ISP).

Azure Traffic Manager - traffic routing methods | Microsoft Learn