

Configure virtual networks

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/1-introduction>

Introduction

Completed

Azure virtual networks are an essential component for creating private networks in Azure. They allow different Azure resources to securely communicate with each other, the internet, and on-premises networks.

Suppose you work for a company in the healthcare industry. Your company is looking to migrate their on-premises infrastructure to Azure. They want to ensure secure communication between their resources in Azure and their on-premises network. The company is also concerned about scalability and availability. By using Azure virtual networks, they can create a private network in Azure and securely connect their resources.

The topics covered in this module include subnetting, creating virtual networks, and using private and public IP addresses. You also learn about the different scenarios where virtual networks can be used. These scenarios include creating a dedicated private cloud-only network or extending a data center securely. The module provides a detailed explanation of subnets and their benefits, and how to plan IP addressing for Azure resources.

By the end of this module, you have a clear understanding of how to create and configure AI-ready virtual networks in Azure. You're able to effectively use subnets, assign IP addresses, and ensure secure communication between your Azure resources and on-premises network.

Learning objectives

In this module, you learn how to:

- Describe Azure virtual network features and components.
- Identify features and usage cases for subnets and subnetting.
- Identify usage cases for private and public IP addresses.
- Create a virtual network and assign an IP address.

Skills measured

The content in the module helps you prepare for [Exam AZ-104: Microsoft Azure Administrator](#).

Prerequisites

- Basic knowledge of virtual networking in cloud environments.
- Familiarity with IP address formats and subnetting.

2. Plan virtual networks

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/2-plan-virtual-networks>

Plan virtual networks

Completed

A major incentive for adopting cloud solutions like Azure is to enable information technology departments to transition server resources to the cloud. Moving resources to the cloud can save money and simplify administrative operations. Relocating resources removes the need to maintain expensive datacenters with uninterruptible power supplies, generators, multiple fail-safes, or clustered database servers. For small and medium-sized companies, which might not have the expertise to maintain their own robust infrastructure, moving to the cloud is particularly appealing.

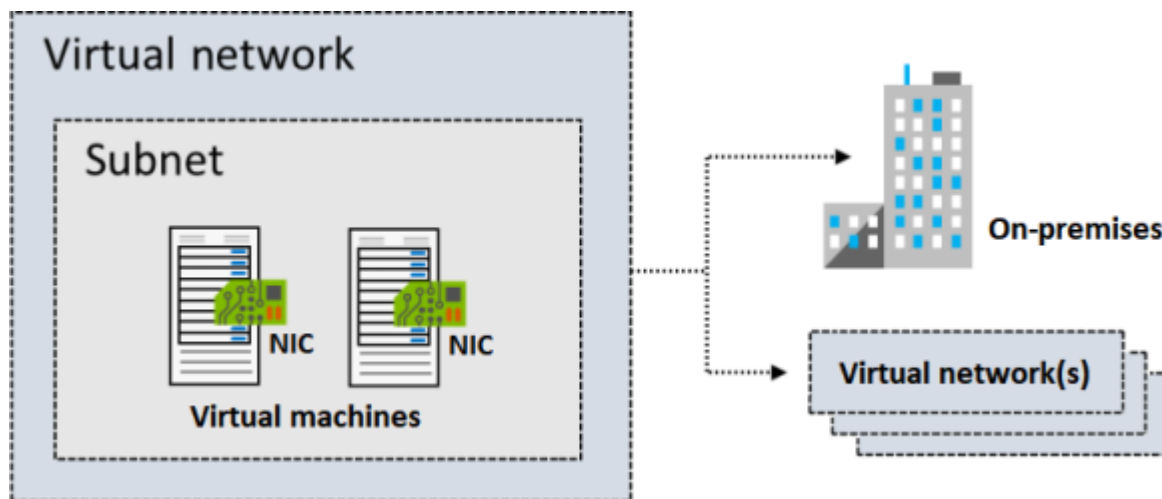
Things to know about Azure virtual networks

You can implement Azure Virtual Network to create a virtual representation of your network in the cloud. With some [planning](#), you can deploy virtual networks and connect the resources you need more effectively. Let's examine some characteristics of virtual networks in Azure.

- An Azure virtual network is a logical isolation of the Azure cloud resources.
- You can use virtual networks to provision and manage virtual private networks (VPNs) in Azure.

- Each virtual network has its own Classless Inter-Domain Routing (CIDR) block and can be linked to other virtual networks and on-premises networks.
- You can link virtual networks with an on-premises IT infrastructure to create hybrid or cross-premises solutions, when the CIDR blocks of the connecting networks don't overlap.
- You control the DNS server settings for virtual networks, and segmentation of the virtual network into subnets.

The next illustration depicts a virtual network that has a subnet containing two virtual machines. The virtual network has connections to an on-premises infrastructure and a separate virtual network.



Things to consider when using virtual networks

Virtual networks can be used in many ways. As you think about the configuration plan for your virtual networks and subnets, consider the following scenarios.

Scenario	Description
<i>Create a dedicated private cloud-only virtual network</i>	Sometimes you don't require a cross-premises configuration for your solution. When you create a virtual network, your services and virtual machines within your virtual network can communicate directly and securely with each other in the cloud. You can still configure endpoint connections for the virtual machines and services that require internet communication, as part of your solution.
<i>Securely extend your data center with virtual networks</i>	You can build traditional site-to-site VPNs to securely scale your datacenter capacity. Site-to-site VPNs use IPSEC to provide a secure connection between your corporate VPN gateway and Azure.
<i>Enable hybrid cloud scenarios</i>	Virtual networks give you the flexibility to support a range of hybrid cloud scenarios. You can securely connect cloud-based applications to any type of on-premises system, such as mainframes and Unix systems.

3. Create subnets

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/3-create-subnets>

Create subnets

Completed

Azure [Subnets](#) provide a way for you to implement logical divisions within your virtual network. Your network can be segmented into subnets to help improve security, increase performance, and make it easier to manage.

Things to know about subnets

There are certain conditions for the IP addresses in a virtual network when you apply segmentation with subnets.

- Each subnet contains a range of IP addresses that fall within the virtual network address space.
- The address range for a subnet must be unique within the address space for the virtual network.
- The range for one subnet can't overlap with other subnet IP address ranges in the same virtual network.
- The IP address space for a subnet must be specified by using CIDR notation.
- You can segment a virtual network into one or more subnets in the Azure portal. Characteristics about the IP addresses for the subnets are listed.

+ Subnet	+ Gateway subnet	Refresh	Manage users	Delete
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	10.0.30.0/26	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

Reserved addresses

For each subnet, Azure reserves five IP addresses. The first four addresses and the last address are reserved.

Let's examine the reserved addresses in an IP address range of `192.168.1.0/24`.

Reserved address	Reason
<code>192.168.1.0</code>	This value identifies the virtual network address.
<code>192.168.1.1</code>	Azure configures this address as the default gateway.
<code>192.168.1.2</code> and <code>192.168.1.3</code>	Azure maps these Azure DNS IP addresses to the virtual network space.
<code>192.168.1.255</code>	This value supplies the virtual network broadcast address.

Things to consider when using subnets

When you plan for adding subnet segments within your virtual network, there are several factors to consider.

- **Consider service requirements.** Each service directly deployed into a virtual network has specific requirements for routing and the types of traffic that must be allowed into and out of associated subnets. A service might require or create their own subnet. There must be enough unallocated space to meet the service requirements. Suppose you connect a virtual network to an on-premises network by using Azure VPN Gateway. The virtual network must have a dedicated subnet for the gateway.
- **Consider network virtual appliances.** Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets. You can also override the default to route traffic between subnets through a network virtual appliance. If you require traffic between resources in the same virtual network to flow through a network virtual appliance, deploy the resources to different subnets.
- **Consider network security groups.** You can associate zero or one network security group to each subnet in a virtual network. You can associate the same or a different network security

group to each subnet. Each network security group contains rules that allow or deny traffic to and from sources and destinations.

- **Consider private links.** Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services. Private Link simplifies the network architecture and secures the connection between endpoints in Azure. The service eliminates data exposure to the public internet.

4. Create virtual networks

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/4-create-virtual-networks>

Create virtual networks

Completed

You can create new virtual networks at any time. You can also add virtual networks when you create a virtual machine.

Things to know about creating virtual networks

Review these requirements for creating a virtual network.

- When you create a virtual network, you need to define the IP address space for the network.
- Plan to use an IP address space that's not already in use in your organization.
- The address space for the virtual network can be either on-premises or in the cloud, but not both.
- To create a virtual network, you need to define at least one subnet.
 - Each subnet contains a range of IP addresses that fall within the virtual network address space.
 - The address range for each subnet must be unique within the address space for the virtual network.
 - The range for one subnet can't overlap with other subnet IP address ranges in the same virtual network.
- You can create a virtual network in the Azure portal. Provide the Azure subscription, resource group, virtual network name, and service region for the network.

Create virtual network ...



Basics IP Addresses Security Tags Review + create

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 is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ

Visual Studio Enterprise



Resource group * ⓘ



[Create new](#)

Instance details

Name *

Region *

West Central US



Note

Default limits on Azure networking resources can change periodically. Be sure to consult the [Azure networking documentation](#) for the latest information.

5. Plan IP addressing

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/5-plan-addressing>

Plan IP addressing

Completed

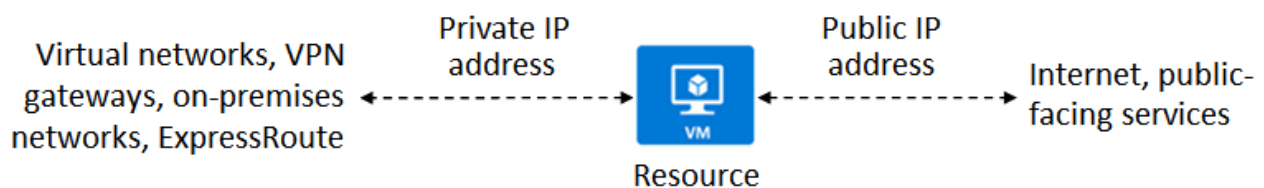
Let's begin with an overview of IP addressing.

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 Azure IP addresses: *private* and *public*.

Private IP addresses enable communication within an Azure virtual network and your on-premises network. You create a private IP address for your resource when you use a VPN gateway or Azure ExpressRoute circuit to extend your network to Azure.

Public IP addresses allow your resource to communicate with the internet. You can create a public IP address to connect with Azure public-facing services.

The next illustration shows a virtual machine resource that has a private IP address and a public IP address.



Things to know about IP addresses

Let's take a closer look at the characteristics of IP addresses.

- IP addresses can be statically assigned or dynamically assigned.
- You can separate dynamically and statically assigned IP resources into different subnets.
- Static IP addresses don't change and are best for certain situations, such as:
 - DNS name resolution, where a change in the IP address requires updating host records.
 - IP address-based security models that require apps or services to have a static IP address.
 - TLS/SSL certificates linked to an IP address.
 - Firewall rules that allow or deny traffic by using IP address ranges.
 - Role-based virtual machines such as Domain Controllers and DNS servers.

6. Create public IP addressing

Create public IP addressing

Completed

You can create a public IP address for your resource in the Azure portal. For example, you could create a public IP address for a virtual machine.

Create public IP address ...

Basics

DDoS Protection

Tags

Review + create

SKU * ⓘ

☐ Standard V2: For use with Standard V2 NAT Gateway

☒ Standard

Availability zone * ⓘ

Zone-redundant

Tier * ⓘ

☒ Regional

☐ Global

IP address assignment

Static IPs are assigned at the time the resource is created and released when the resource is deleted.

IP address assignment *

Static

Things to consider when creating a public IP address

To create a public IP address, configure these settings. Notice that public IP addresses are often used with load balancers.

- **IP Version:** Public IP addresses can be attached to a load balancer or to a network interface. IPv4 and IPv6 addresses are charged at the same rate.
- **SKU:** Select the SKU for the public IP address. A Public IP's SKU must match the SKU of the Load Balancer with which it is used.
- **Tier:** Must match the load balancer tier. A cross-region load balancer distributes traffic across regional backends. Regional distributes traffic within a virtual network.

- **IP address assignment:** Static addresses are assigned when a public IP address is created. Static addresses aren't released until a public IP address resource is deleted.

7. Associate public IP addresses

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/7-associate-public-ip-addresses>

Associate public IP addresses

Completed

A [public IP address](#) resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways. You can associate your resource with both dynamic and static public IP addresses.

Things to consider when associating public IP addresses

The next table summarizes how you can associate public IP addresses for different types of resources.

Top-level resource	IP address configuration
Virtual machine	Network interface configuration
Virtual Network Gateway (VPN), Virtual Network Gateway (ER), NAT Gateway	Gateway IP configuration
Public Load Balancer, Application Gateway, Azure Firewall, Route Server, API Management	Front-end configuration
Bastion host	Public IP configuration

Public IP address SKU features

The next table summarizes the standard SKU features.

Public IP address	Standard SKU
Allocation method	Static
Security	Secure by default model
Available zones	Supported. Standard IPs can be nonzonal, zonal, or zone-redundant.

8. Allocate or assign private IP addresses

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/8-associate-private-ip-addresses>

Allocate or assign private IP addresses

Completed

A [private IP address](#) resource can be associated with virtual machine network interfaces, internal load balancers, and application gateways. Azure can provide an IP address (dynamic assignment) or you can assign the IP address (static assignment).

Things to consider when associating private IP addresses

The next table summarizes how you can associate private IP addresses for different types of resources.

Resource	Private IP address association	Dynamic IP address	Static IP address
Virtual machine	NIC	Yes	Yes
Internal load balancer	Front-end configuration	Yes	Yes
Application gateway	Front-end configuration	Yes	Yes

Private IP address assignment

A private IP address is allocated from the address range of the virtual network subnet that a resource is deployed in. There are two options: dynamic and static.

- **Dynamic:** Azure assigns the next available unassigned or unreserved IP address in the subnet's address range. Dynamic assignment is the default allocation method.

Suppose addresses 10.0.0.4 through 10.0.0.9 are already assigned to other resources. In this case, Azure assigns the address 10.0.0.10 to a new resource.

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

Suppose a subnet's address range is 10.0.0.0/16, and addresses 10.0.0.4 through 10.0.0.9 are already assigned to other resources. In this scenario, you can assign any address between 10.0.0.10 and 10.0.255.254.

Tip

For a more complete review of virtual networks, consider the [Introduction to Virtual Networks](#) training module.

9. Exercise: Create and configure virtual networks

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/9-simulation-create-networks>

Exercise: Create and configure virtual networks

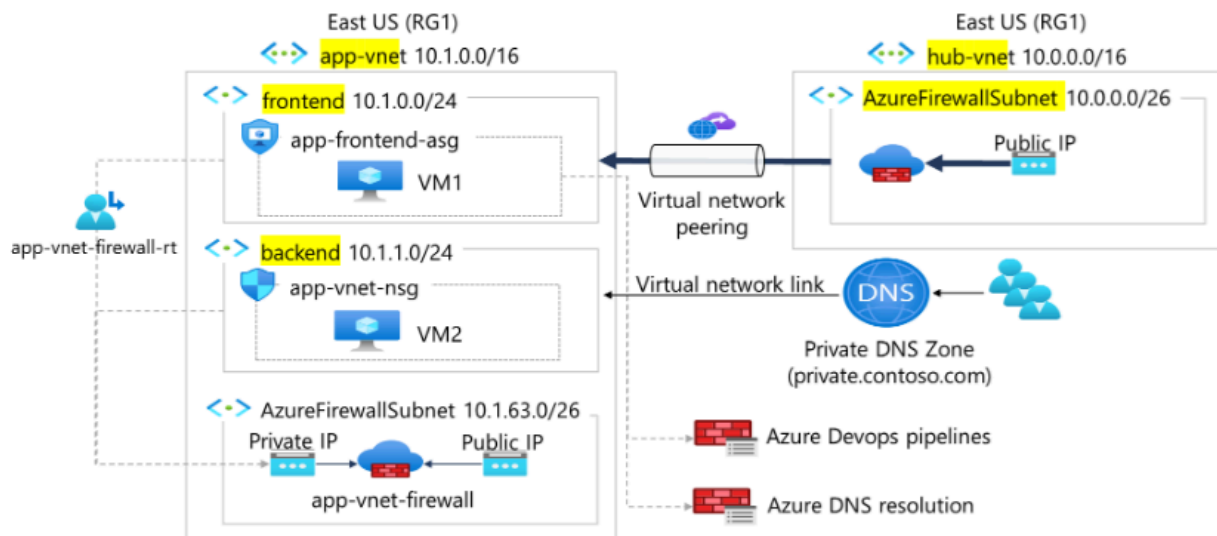
Completed

Exercise scenario

Your organization is migrating a web-based application to Azure. Your first task is to put in place the virtual networks and subnets. You also need to securely peer the virtual networks. You identify these requirements.

- Two virtual networks are required, app-vnet and hub-vnet. The virtual networks simulate a hub and spoke network architecture.
- The app-vnet hosts the application. The app-vnet virtual network requires two subnets. The frontend subnet hosts the web servers. The backend subnet hosts the database servers.
- The hub-vnet only requires a subnet for the firewall.
- The two virtual networks must be able to communicate with each other securely and privately through virtual network peering.
- Both virtual networks should be in the same region.

Architecture diagram



Job skills

- Create a virtual network.
- Create a subnet.
- Configure virtual network peering (optional).

Note

Estimated time: 30 minutes. To complete this exercise, you need an [Azure subscription](#).

Launch the exercise, and follow the instructions. When finished, be sure to return to this page so you can continue learning.

[Launch Exercise](#)

10. Module assessment

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/10-knowledge-check>

Module assessment

Completed

11. Summary and resources

<https://learn.microsoft.com/en-us/training/modules/configure-virtual-networks/11-summary-resources>

Summary and resources

Completed

In this module, you learned about Azure virtual networks and their importance in creating private networks in Azure. You explored the benefits of using virtual networks, such as scalability, availability, and isolation. You learned how to create virtual networks with subnetting and how to determine which resources require public or private IP addresses.

The main takeaways from this module are:

- Azure virtual networks allow different Azure resources to securely communicate with each other, the internet, and on-premises networks.
- Subnets within virtual networks provide logical divisions, improving security, performance, and management.
- When creating virtual networks, ensure that the IP address space is unique and doesn't overlap with other subnets.
- IP addresses can provide public or private access to resources.

Learn more with Copilot

Copilot can assist you in designing Azure infrastructure solutions. Copilot can compare, recommend, explain, and research products and services where you need more information. Open a Microsoft Edge browser and choose Copilot (top right) or navigate to copilot.microsoft.com. Take a few minutes to try these prompts and extend your learning with Copilot.

- Explain CIDR for a nontechnical audience. Provide examples.
- What are the basic steps and considerations for creating a virtual network in Azure?
- What types of Azure resources should be assigned a static IP address?

Learn more with documentation

- [What is Azure Virtual Network?](#). This article is your starting point to learn about virtual networks.

- [Public IP addresses](#). This article reviews the basics of when to use public IP addresses.
- [Private IP addresses](#). This article reviews the basics of when to use private IP addresses.

Learn more with self-paced training

- [Introduction to Azure Virtual Networks](#). Learn how to design and implement core Azure Networking infrastructure.
- [Implement Windows Server IaaS virtual machine IP addressing and routing](#). Learn about IP addressing and virtual networks for virtual machines.