

Configure Azure Virtual Network peering

1. Introduction

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

Introduction

Completed

Azure Virtual Network peering lets you connect virtual networks in the same or different regions. Azure Virtual Network peering provides secure communication between resources in the peered networks.

Suppose your engineering company is migrating services to Azure. The company is deploying services into separate Azure virtual networks. Private connectivity between the virtual networks isn't yet configured. Several business units identified services in the virtual networks that need to communicate with each other.

You're responsible for implementing an Azure Virtual Network peering solution and enabling connectivity between the virtual networks. Two of your strategy goals include preventing exposure of the services to the internet, and keeping the integration as simple as possible. Your solution should address transit and connectivity concerns.

The goal of this module is to successfully implement Azure Virtual Network peering.

Learning objectives

In this module, you learn how to:

- Identify usage cases and product features of Azure Virtual Network peering.
- Configure your network to implement Azure VPN Gateway for transit connectivity.
- Extend peering by using a hub and spoke network with user-defined routes and service chaining.

Skills measured

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

Prerequisites

- Basic understanding of cloud networking including virtual networks and virtual machines.
- Familiarity with the command line connectivity testing tools.

2. Determine Azure Virtual Network peering uses

<https://learn.microsoft.com/en-us/training/modules/configure-vnet-peering/2-determine-uses>

Determine Azure Virtual Network peering uses

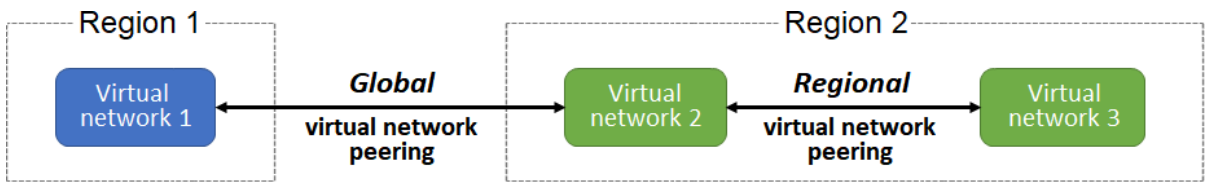
Completed

Perhaps the simplest and quickest way to connect your virtual networks is to use Azure Virtual Network peering. Virtual Network peering enables you to seamlessly connect two Azure virtual networks. After the networks are peered, the two virtual networks operate as a single network, for connectivity purposes.

Things to know about Azure Virtual Network peering

Let's examine some prominent characteristics of Azure Virtual Network peering.

- There are two types of Azure Virtual Network peering: *regional* and *global*.



- **Regional virtual network peering** connects Azure virtual networks that exist in the same region.
- **Global virtual network peering** connects Azure virtual networks that exist in different regions.
- You can create a regional peering of virtual networks in the same Azure public cloud region, or in the same China cloud region, or in the same Microsoft Azure Government cloud region.
- You can create a global peering of virtual networks in any Azure public cloud region, or in any China cloud region.
- Global peering of virtual networks in different Azure Government cloud regions isn't permitted.
- After you create a peering between virtual networks, the individual virtual networks are still managed as separate resources.
- Virtual networks can be peered across subscriptions and tenants.

Things to consider when using Azure Virtual Network peering

Consider the benefits of using Azure Virtual Network peering.

Benefit	Description
Private network connections	When you implement Azure Virtual Network peering, network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft Azure backbone network. No public internet, gateways, or encryption is required in the communication between the virtual networks.
Strong performance	Because Azure Virtual Network peering utilizes the Azure infrastructure, you gain a low-latency, high-bandwidth connection between resources in different virtual networks.
Simplified communication	Azure Virtual Network peering lets resources in one virtual network communicate with resources in a different virtual network, after the virtual networks are peered.
Seamless data transfer	You can create an Azure Virtual Network peering configuration to transfer data across Azure subscriptions, deployment models, and across Azure regions.
No resource disruptions	Azure Virtual Network peering doesn't require downtime for resources in either virtual network when creating the peering, or after the peering is created.

Things to know about peering requirements and limitations

While VNet peering provides many benefits, there are important constraints to understand.

Requirements/Limitations	Description
Nonoverlapping address spaces	Peered virtual networks must have non-overlapping IP address spaces. Peering creation fails if address ranges overlap.
Address space modification restrictions	If you want to change a VNet's address range, you need to delete the peering first, update the address space, and then set up the peering again.
Basic Load Balancer limitations	Resources in one VNet can't communicate with Basic Internal Load Balancer IPs in VNets peered across regions. Use the Standard Load Balancer for cross-region connections.
DNS resolution boundaries	Azure's built-in name resolution does not work across peered VNets. Configure Azure Private DNS zones or custom DNS servers for cross-VNet name resolution.

3. Determine gateway transit and connectivity

<https://learn.microsoft.com/en-us/training/modules/configure-vnet-peering/3-determine-gateway-transit-connectivity>

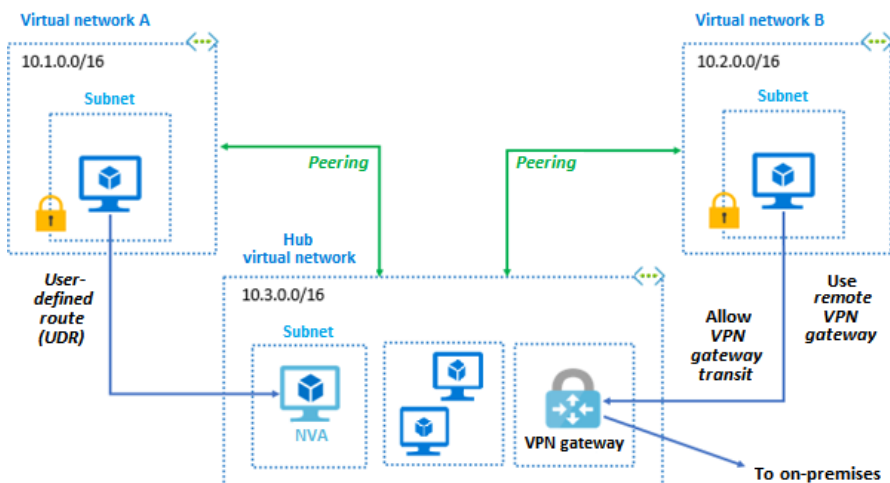
Determine gateway transit and connectivity

Completed

When virtual networks are peered, you can configure Azure VPN Gateway in the peered virtual network as a *transit point*. In this scenario, a peered virtual network uses the remote VPN gateway to gain access to other resources.

Transit and connectivity use

Consider a scenario where three virtual networks in the same region are connected by virtual network peering. Virtual network A and virtual network B are each peered with a hub virtual network. The hub virtual network contains several resources, including a gateway subnet and an Azure VPN gateway. The VPN gateway is configured to allow VPN gateway transit. Virtual network B accesses resources in the hub, including the gateway subnet, by using a remote VPN gateway.



The Azure portal provides four key settings when configuring virtual network peering.

Add peering

...



vnet-1

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. This will allow resources in either virtual network to directly connect and communicate with resources in the peered virtual network.

Remote virtual network summary

Peering link name *

vnet-2-to-vnet-1

Remote virtual network peering settings

Allow 'vnet-2' to access 'vnet-1' ⓘ



Allow 'vnet-2' to receive forwarded traffic from 'vnet-1' ⓘ



Allow gateway or route server in 'vnet-2' to forward traffic to 'vnet-1' ⓘ



Enable 'vnet-2' to use 'vnet-1's' remote gateway or route server ⓘ



- **Traffic to remote virtual network.** Controls whether traffic flows from this VNet to the remote VNet.
- **Traffic forwarded from remote virtual network.** Controls whether forwarded (non-originating) traffic is accepted from the peered VNet.
- **Virtual network gateway or Route Server.** Enables gateway transit. Lets peered VNets use this VNet's VPN Gateway or Azure Route Server.
- **Remote virtual network gateway or Route Server.** Enables this VNet to use the remote VNet's VPN Gateway or Route Server.

Things to know about Azure VPN Gateway

Let's take a closer look at how Azure VPN Gateway is implemented with Azure Virtual Network peering.

- A virtual network can have only one VPN gateway.
- Gateway transit is supported for both regional and global virtual network peering.
- When you allow VPN gateway transit, the virtual network can communicate to resources outside the peering. In our sample illustration, the gateway subnet gateway within the hub virtual network can complete tasks such as:
 - Use a site-to-site VPN to connect to an on-premises network.
 - Use a vnet-to-vnet connection to another virtual network.
 - Use a point-to-site VPN to connect to a client.
- Gateway transit allows peered virtual networks to share the gateway and get access to external resources. With this implementation, you don't need to deploy a VPN gateway in the peered virtual network.
- You can apply network security groups in a virtual network to block or allow access to other virtual networks or subnets. When you configure virtual network peering, you can choose to open or close the network security group rules between the virtual networks.

4. Create virtual network peering

Create virtual network peering

Completed

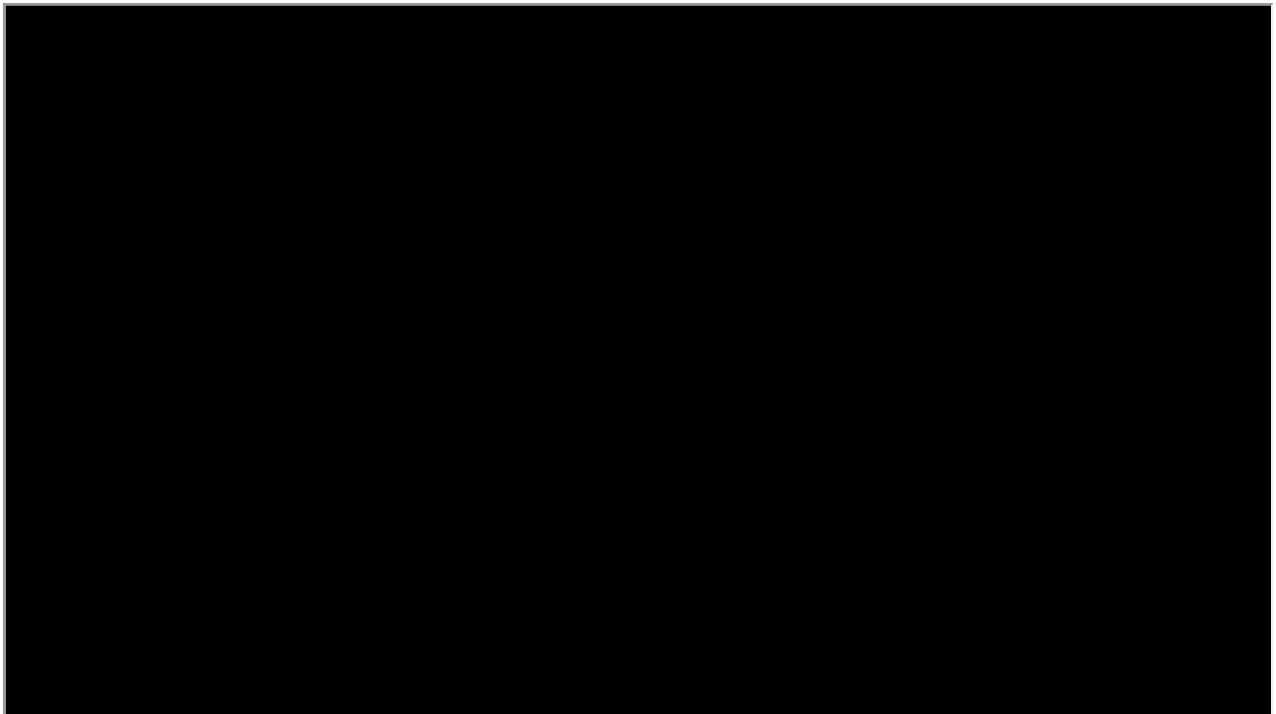
Azure Virtual Network peering can be configured for virtual networks by using PowerShell, the Azure CLI, and in the Azure portal. In this module, we review the steps to create the peering in the Azure portal for virtual networks deployed through Azure Resource Manager.

Things to know about creating virtual network peering

There are a few points to review before we look at how to create the peering in the Azure portal.

- To implement virtual network peering, your Azure account must be assigned to the **Network Contributor** role. Alternatively, your Azure account can be assigned to a custom role that can complete the necessary peering actions. For details, see [Permissions](#).
- To create a peering, you need two virtual networks.
- The second virtual network in the peering is referred to as the *remote network*.
- Initially, the virtual machines in your virtual networks can't communicate with each other. After the peering is established, the machines can communicate within the peered network based on your configuration settings.

How to connect virtual networks across Azure regions with Azure Global virtual network peering



How to check your peering status

In the Azure portal, you can check the connectivity status of the virtual networks in your virtual network peering. The status conditions depend on how your virtual networks are deployed.

Important

Your peering isn't successfully established until both virtual networks in the peering have a status of **Connected**.

- The two peering status conditions are **Initiated** and **Connected**.
- When you create the initial peering to the second (remote) virtual network from the first virtual network, the peering status for the first virtual network is **Initiated**.

5. Extend peering with user-defined routes and service chaining

<https://learn.microsoft.com/en-us/training/modules/configure-vnet-peering/5-determine-service-chaining-uses>

Extend peering with user-defined routes and service chaining

Completed

Virtual network peering is nontransitive. The communication capabilities in a peering are available to only the virtual networks and resources in the peering. Other mechanisms have to be used to enable traffic to and from resources and networks outside the private peering network.

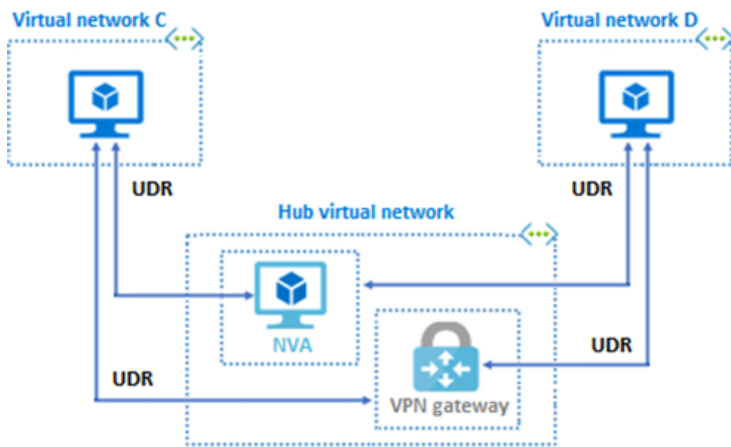
Suppose you have three virtual networks: A, B, and C. You establish virtual network peering between networks A and B, and also between networks B and C. You don't set up peering between networks A and C. The virtual network peering capabilities that you set up between networks B and C don't automatically enable peering communication capabilities between networks A and C.

Things to know about extending peering

There are a few ways to extend the capabilities of your peering for resources and virtual networks outside your peering network.

Mechanism	Description
Hub and spoke network	When you deploy a hub-and-spoke network, the hub virtual network can host infrastructure components like a network virtual appliance (NVA) or Azure VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic can flow through NVAs or VPN gateways in the hub virtual network.
User-defined route (UDR)	Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway.
Service chaining	Service chaining is used to direct traffic from one virtual network to a virtual appliance or gateway. To enable service chaining, configure UDRs that point to virtual machines in peered virtual networks as the next hop IP address. UDRs could also point to virtual network gateways to enable service chaining.
Azure Virtual Network Manager	Centrally manages hub-and-spoke or mesh peering topologies at scale. Automates peering creation without manual per-VNet configuration.

The following diagram shows a hub and spoke virtual network with an NVA and VPN gateway. The hub and spoke network is accessible to other virtual networks via user-defined routes and service chaining.



Tip

Use the **Ask Learn** icon (top right) to learn more about *service chaining and user-defined routes*.

6. Exercise - Implement Intersite Connectivity

<https://learn.microsoft.com/en-us/training/modules/configure-vnet-peering/6-simulation-peering>

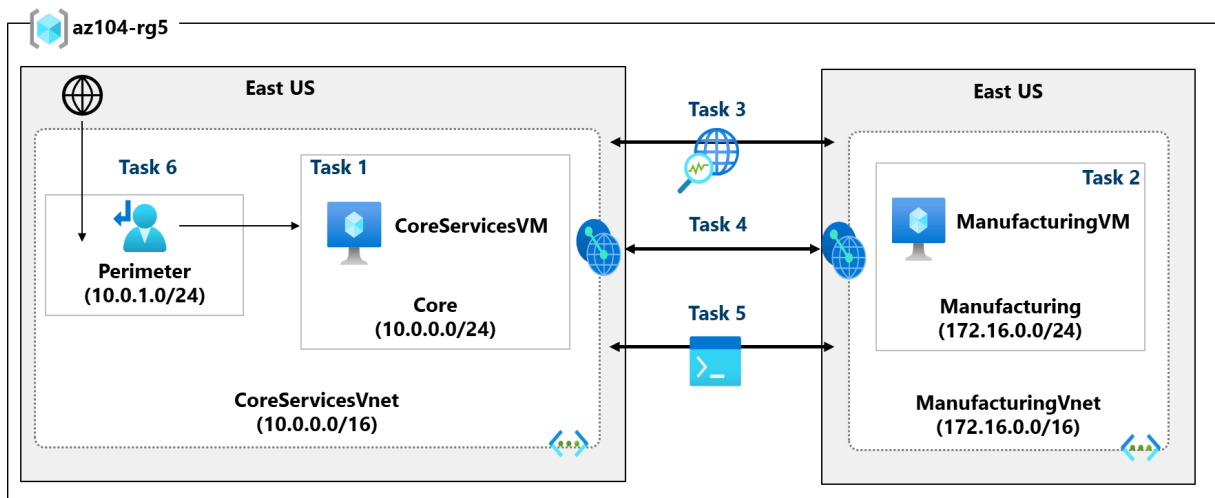
Exercise - Implement Intersite Connectivity

Completed

Lab scenario

Your organization segments core IT apps and services (such as DNS and security services) from other parts of the business, including your manufacturing department. However, in some scenarios, apps and services in the core area need to communicate with apps and services in the manufacturing area. In this lab, you configure connectivity between the segmented areas. Separating production from development or separating one subsidiary from another is a common networking scenario.

Architecture diagram



Job skills

- Create a virtual machine in a virtual network.
- Create a virtual machine in a different virtual network.
- Use Network Watcher to test the connection between virtual machines.
- Configure virtual network peerings between different virtual networks.
- Use Azure PowerShell to test the connection between virtual machines.
- Create a custom route. (optional)

Important

Estimated time: 50 minutes. To complete the 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

7. Module assessment

<https://learn.microsoft.com/en-us/training/modules/configure-vnet-peering/7-knowledge-check>

Module assessment

Completed

8. Summary and resources

<https://learn.microsoft.com/en-us/training/modules/configure-vnet-peering/8-summary-resources>

Summary and resources

Completed

In this module, you learned Azure Virtual Network peering lets you connect virtual networks in a hub and spoke topology. You learned how to configure your virtual networks with Azure VPN Gateway for transit connectivity. You explored how to extend peering with user-defined routes and service chaining.

The main takeaways from this module are:

- Azure Virtual Network peering allows for the connection of virtual networks in a hub and spoke topology.
- There are two types of peering: regional and global. Regional peering connects virtual networks in the same region. Global peering connects virtual networks in different regions.
- Network traffic between peered virtual networks is private and kept on the Azure backbone network.
- You can configure Azure VPN Gateway in the peered virtual network as a transit point to access resources in another network.
- Network security groups can be applied to block or allow access between virtual networks when configuring virtual network peering.

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.

- What is Azure virtual network peering and what are the advantages of this feature?
- What are some of the configurations settings for Azure virtual network peering?

Learn more with documentation

- [Azure Virtual Network peering](#). This article is your starting point for learning about virtual network peering.
- [Create, change, or delete a virtual network peering](#). This article reviews how to create a virtual network peering and what each setting means.

Learn more with self-paced training

- [Introduction to Azure Virtual Networks](#). Learn how to design and implement core Azure networking infrastructure such as virtual networks, and virtual network peering.