**Azure Network**

What is Azure Virtual Network?

Azure Virtual Network enables Azure resources to communicate with each other and the internet. A virtual network isolates your resources from others' resources in the Azure cloud. You can connect virtual networks to other virtual networks, or to your on-premises network.

Azure Virtual Network provides the following broad capabilities:

* [**Isolation:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#isolation) Virtual networks are isolated from one another. You can create separate virtual networks for development, testing, and production that use the same CIDR (10.0.0.0/0, for example) address blocks. Conversely, you can create multiple virtual networks that use different CIDR address blocks and connect the networks together. You can segment a virtual network into multiple subnets. Azure provides internal name resolution for resources deployed in a virtual network. If necessary, you can configure a virtual network to use your own DNS servers, instead of using Azure internal name resolution.
* [**Internet communication:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#internet) Resources, such as virtual machines deployed in a virtual network, have access to the Internet, by default. You can also enable inbound access to specific resources, as needed.
* [**Azure resource communication:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#within-vnet) Azure resources deployed in a virtual network can communicate with each other using private IP addresses, even if the resources are deployed in different subnets. Azure provides default routing between subnets, connected virtual networks, and on-premises networks, so you don't have to configure and manage routes. If desired, you can customize Azure's routing.
* [**Virtual network connectivity:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#connect-vnets) Virtual networks can be connected to each other, enabling **resources in any virtual network to communicate** with resources in any other virtual network.
* [**On-premises connectivity:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#connect-on-premises) A virtual network can be connected to an on-premises network, enabling resources to communicate between each other.
* [**Traffic filtering:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#filtering) You can filter network traffic to and from resources in a virtual network by source IP address and port, destination IP address and port, and protocol.
* [**Routing:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#routing) You can optionally override Azure's default routing by configuring your own routes, or by propagating border gateway protocol (BGP) routes through a network gateway.

## Network isolation and segmentation

You can implement multiple virtual networks within each Azure [subscription](https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#subscription) and Azure [region](https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#region). Each virtual network is isolated from other virtual networks. For each virtual network you can:

* Specify a custom private IP address space using public and private (RFC 1918) addresses. Azure assigns resources in a virtual network a private IP address from the address space you assign.
* Segment the virtual network into one or more subnets and allocate a portion of the virtual network's address space to each subnet.
* Use Azure-provided name resolution, or specify your own DNS server, for use by resources in a virtual network. To learn more about name resolution in virtual networks, see [Name resolution for resources in virtual networks](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances).

## Connect to an on-premises network

You can connect your on-premises network to a virtual network using any combination of the following options:

* **Point-to-site virtual private network (VPN):** Established between a virtual network and a single PC in your network. Each PC that wants to establish connectivity with a virtual network must configure its connection independently. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The connection uses the SSTP protocol to provide encrypted communication over the Internet between the PC and a virtual network. The latency for a point-to-site VPN is unpredictable, since the traffic traverses the Internet.
* **Site-to-site VPN:** Established between your VPN device and an Azure VPN Gateway deployed in a virtual network. This connection type enables any on-premises resource you authorize to access a virtual network. The connection is an IPSec/IKE VPN that provides encrypted communication over the Internet between your on-premises device and the Azure VPN gateway. The latency for a site-to-site connection is unpredictable, since the traffic traverses the Internet.
* **Azure ExpressRoute:** Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not traverse the Internet. The latency for an ExpressRoute connection is predictable, since traffic doesn't traverse the Internet.

## Filter network traffic

You can filter network traffic between subnets using either or both of the following options:

* **Network security groups:** A network security group can contain multiple inbound and outbound security rules that enable you to filter traffic by source and destination IP address, port, and protocol. You can apply a network security group to each network interface in a virtual machine. You can also apply a network security group to the subnet a network interface, or other Azure resource, is in. To learn more about network security groups, see [Network security groups](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups).
* **Network virtual appliances:** A network virtual appliance is a virtual machine running software that performs a network function, such as a firewall. View a list of available network virtual appliances in the [Azure Marketplace](https://azuremarketplace.microsoft.com/marketplace/apps/category/networking?page=1&subcategories=appliances). Network virtual appliances are also available that provide WAN optimization and other network traffic functions. Network virtual appliances are typically used with user-defined or BGP routes. You can also use a network virtual appliance to filter traffic between virtual networks.

## Route network traffic

Azure creates route tables that enable resources connected to any subnet in any virtual network to communicate with each other, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

* **Route tables:** You can create custom route tables with routes that control where traffic is routed to for each subnet. To learn more about custom routing, see [Custom routing](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#user-defined).
* **BGP routes:** If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate BGP routes to your virtual networks.

# Create, change, or delete a virtual network

## reate a virtual network

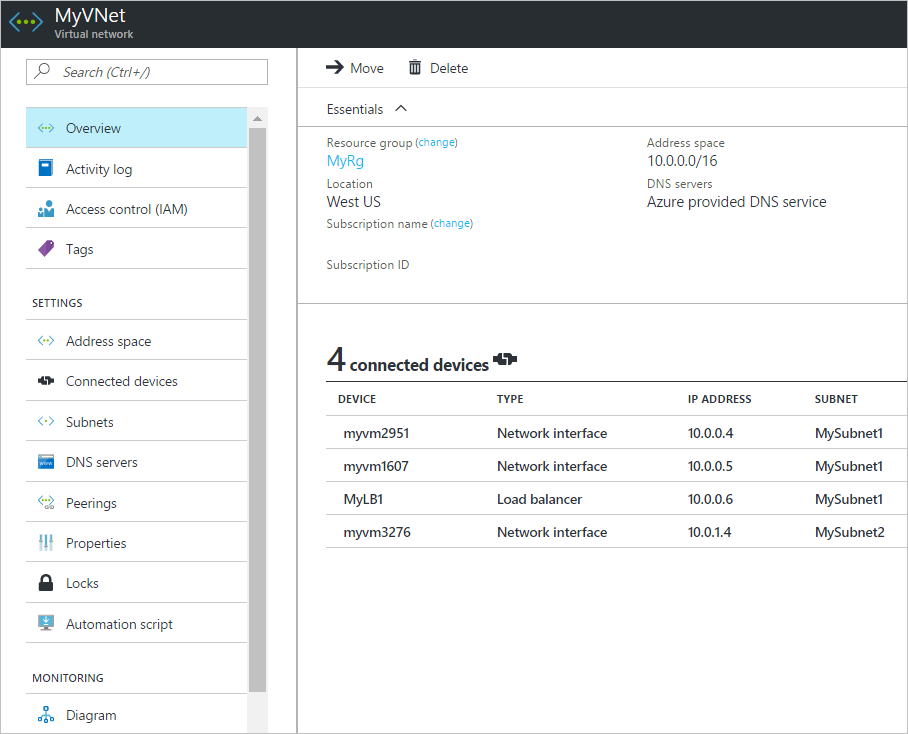
1. Select **+ Create a resource** > **Networking** > **Virtual network**.
2. Enter or select values for the following settings, then select **Create**:
   * **Name**: The name must be unique in the [resource group](https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#resource-group) that you select to create the virtual network in. You cannot change the name after the virtual network is created. You can create multiple virtual networks over time. For naming suggestions, see [Naming conventions](https://docs.microsoft.com/en-us/azure/architecture/best-practices/naming-conventions.md?toc=%2fazure%2fvirtual-network%2ftoc.json#naming-rules-and-restrictions). Following a naming convention can help make it easier to manage multiple virtual networks.
   * **Address space**: The address space for a virtual network is composed of one or more non-overlapping address ranges that are specified in CIDR notation. The address range you define can be public or private (RFC 1918). Whether you define the address range as public or private, the address range is reachable only from within the virtual network, from interconnected virtual networks, and from any on-premises networks that you have connected to the virtual network. You cannot add the following address ranges:
     + 224.0.0.0/4 (Multicast)
     + 255.255.255.255/32 (Broadcast)
     + 127.0.0.0/8 (Loopback)
     + 169.254.0.0/16 (Link-local)
     + 168.63.129.16/32 (Internal DNS)

**Subnet name**: The subnet name must be unique within the virtual network. You cannot change the subnet name after the subnet is created. The portal requires that you define one subnet when you create a virtual network, even though a virtual network isn't required to have any subnets. In the portal, you can define only one subnet when you create a virtual network. You can add more subnets to the virtual network later, after the virtual network is created. To add a subnet to a virtual network, see [Manage subnets](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet). You can create a virtual network that has multiple subnets by using Azure CLI or PowerShell.

* **Subnet address range**: The range must be within the address space you entered for the virtual network. The smallest range you can specify is /29, which provides eight IP addresses for the subnet. Azure reserves the first and last address in each subnet for protocol conformance. Three additional addresses are reserved for Azure service usage. As a result, a virtual network with a subnet address range of /29 has only three usable IP addresses. If you plan to connect a virtual network to a VPN gateway, you must create a gateway subnet. Learn more about [specific address range considerations for gateway subnets](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings?toc=%2fazure%2fvirtual-network%2ftoc.json#gwsub). You can change the address range after the subnet is created, under specific conditions. To learn how to change a subnet address range, see [Manage subnets](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet).
* **Subscription**: Select a [subscription](https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#subscription). You cannot use the same virtual network in more than one Azure subscription. However, you can connect a virtual network in one subscription to virtual networks in other subscriptions with [virtual network peering](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview). Any Azure resource that you connect to the virtual network must be in the same subscription as the virtual network.
* **Resource group**: Select an existing [resource group](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview?toc=%2fazure%2fvirtual-network%2ftoc.json#resource-groups) or create a new one. An Azure resource that you connect to the virtual network can be in the same resource group as the virtual network or in a different resource group.
* **Location**: Select an Azure [location](https://azure.microsoft.com/regions/), also known as a region. A virtual network can be in only one Azure location. However, you can connect a virtual network in one location to a virtual network in another location by using a VPN gateway. Any Azure resource that you connect to the virtual network must be in the same location as the virtual network.

## View virtual networks and settings

1. In the search box at the top of the portal, enter virtual networks in the search box. When **Virtual networks**appears in the search results, select it.
2. From the list of virtual networks, select the virtual network that you want to view settings for.
3. The following settings are listed for the virtual network you selected:
   * **Overview**: Provides information about the virtual network, including address space and DNS servers. The following screenshot shows the overview settings for a virtual network named **MyVNet**:



You can move a virtual network to a different subscription or resource group by selecting **Change** next to **Resource group** or **Subscription name**. To learn how to move a virtual network, see [Move resources to a different resource group or subscription](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-move-resources?toc=%2fazure%2fvirtual-network%2ftoc.json). The article lists prerequisites, and how to move resources by using the Azure portal, PowerShell, and Azure CLI. All resources that are connected to the virtual network must move with the virtual network.

* + **Address space**: The address spaces that are assigned to the virtual network are listed. To learn how to add and remove an address range to the address space, complete the steps in [Add or remove an address range](https://docs.microsoft.com/en-us/azure/virtual-network/manage-virtual-network#add-or-remove-an-address-range).
  + **Connected devices**: Any resources that are connected to the virtual network are listed. In the preceding screenshot, three network interfaces and one load balancer are connected to the virtual network. Any new resources that you create and connect to the virtual network are listed. If you delete a resource that was connected to the virtual network, it no longer appears in the list.
  + **Subnets**: A list of subnets that exist within the virtual network is shown. To learn how to add and remove a subnet, see [Manage subnets](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet).
  + **DNS servers**: You can specify whether the Azure internal DNS server or a custom DNS server provides name resolution for devices that are connected to the virtual network. When you create a virtual network by using the Azure portal, Azure's DNS servers are used for name resolution within a virtual network, by default. To modify the DNS servers, complete the steps in [Change DNS servers](https://docs.microsoft.com/en-us/azure/virtual-network/manage-virtual-network#change-dns-servers)in this article.
  + **Peerings**: If there are existing peerings in the subscription, they are listed here. You can view settings for existing peerings, or create, change, or delete peerings. To learn more about peerings, see [Virtual network peering](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview).
  + **Properties**: Displays settings about the virtual network, including the virtual network's resource ID and the Azure subscription it is in.
  + **Diagram**: The diagram provides a visual representation of all devices that are connected to the virtual network. The diagram has some key information about the devices. To manage a device in this view, in the diagram, select the device.
  + **Common Azure settings**: To learn more about common Azure settings, see the following information:
    - [Activity log](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview?toc=%2fazure%2fvirtual-network%2ftoc.json#activity-logs)
    - [Access control (IAM)](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview?toc=%2fazure%2fvirtual-network%2ftoc.json#access-control)
    - [Tags](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview?toc=%2fazure%2fvirtual-network%2ftoc.json#tags)
    - [Locks](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources?toc=%2fazure%2fvirtual-network%2ftoc.json)
    - [Automation script](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template?toc=%2fazure%2fvirtual-network%2ftoc.json#export-the-template-from-resource-group)

## Add or remove an address range

You can add and remove address ranges for a virtual network. An address range must be specified in CIDR notation, and cannot overlap with other address ranges within the same virtual network. The address ranges you define can be public or private (RFC 1918). Whether you define the address range as public or private, the address range is reachable only from within the virtual network, from interconnected virtual networks, and from any on-premises networks that you have connected to the virtual network. You cannot add the following address ranges:

* 224.0.0.0/4 (Multicast)
* 255.255.255.255/32 (Broadcast)
* 127.0.0.0/8 (Loopback)
* 169.254.0.0/16 (Link-local)
* 168.63.129.16/32 (Internal DNS)

To add or remove an address range:

1. In the search box at the top of the portal, enter virtual networks in the search box. When **Virtual networks**appears in the search results, select it.
2. From the list of virtual networks, select the virtual network for which you want to add or remove an address range.
3. Select **Address space**, under **SETTINGS**.
4. Complete one of the following options:
   * **Add an address range**: Enter the new address range. The address range cannot overlap with an existing address range that is defined for the virtual network.
   * **Remove an address range**: On the right of the address range you want to remove, select **...**, then select **Remove**. If a subnet exists in the address range, you cannot remove the address range. To remove an address range, you must first delete any subnets (and any resources in the subnets) that exist in the address range.
5. Select **Save**.

## Add or remove an address range

You can add and remove address ranges for a virtual network. An address range must be specified in CIDR notation, and cannot overlap with other address ranges within the same virtual network. The address ranges you define can be public or private (RFC 1918). Whether you define the address range as public or private, the address range is reachable only from within the virtual network, from interconnected virtual networks, and from any on-premises networks that you have connected to the virtual network. You cannot add the following address ranges:

* 224.0.0.0/4 (Multicast)
* 255.255.255.255/32 (Broadcast)
* 127.0.0.0/8 (Loopback)
* 169.254.0.0/16 (Link-local)
* 168.63.129.16/32 (Internal DNS)

To add or remove an address range:

1. In the search box at the top of the portal, enter virtual networks in the search box. When **Virtual networks**appears in the search results, select it.
2. From the list of virtual networks, select the virtual network for which you want to add or remove an address range.
3. Select **Address space**, under **SETTINGS**.
4. Complete one of the following options:
   * **Add an address range**: Enter the new address range. The address range cannot overlap with an existing address range that is defined for the virtual network.
   * **Remove an address range**: On the right of the address range you want to remove, select **...**, then select **Remove**. If a subnet exists in the address range, you cannot remove the address range. To remove an address range, you must first delete any subnets (and any resources in the subnets) that exist in the address range.
5. Select **Save**.