Capabilities of Azure Virtual Networks
Azure VNets enable resources in Azure to securely communicate with each other, the internet, and on-premises networks.

Communication with the internet. All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use public IP or public Load Balancer to manage your outbound connections.
Communication between Azure resources. There are three key mechanisms through which Azure resource can communicate: VNets, VNet service endpoints, and VNet peering. Virtual Networks can connect not only virtual machines (VMs), but other Azure Resources, such as the App Service Environment, Azure Kubernetes Service, and Azure Virtual Machine Scale Sets. You can use service endpoints to connect to other Azure resource types, such as Azure SQL databases and storage accounts. When you create a VNet, your services and VMs within your VNet can communicate directly and securely with each other in the cloud.
Communication between on-premises resources. Securely extend your data center. You can connect your on-premises computers and networks to a virtual network using any of the following options: Point-to-site virtual private network (VPN), Site-to-site VPN, Azure ExpressRoute.
Filtering network traffic. You can filter network traffic between subnets using any combination of network security groups and network virtual appliances.
Routing network traffic. Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement route tables or border gateway protocol (BGP) routes to override the default routes Azure creates.
Design considerations for Azure Virtual Networks
Address space and subnets
You can create multiple virtual networks per region per subscription. You can create multiple subnets within each virtual network.

Virtual Networks

When you're creating a VNet, use address ranges enumerated in RFC 1918. These addresses are for private, nonroutable address spaces.

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
In addition, these address ranges are reserved.

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)
Subnets

A subnet is a range of IP address in the VNet. You segment VNets into different size subnets. You then deploy Azure resources in a specific subnet. Just like in a traditional network, subnets allow you to segment your VNet address space into segments that are appropriate for the organization's internal network. The smallest supported IPv4 subnet is /29, and the largest is /2 (using CIDR subnet definitions). IPv6 subnets must be exactly /64 in size. When planning to implement subnets, consider:

Each subnet must have a unique address range, specified in Classless Inter-Domain Routing (CIDR) format.
Certain Azure services require their own subnet.
Subnets can be used for traffic management. For example, you can create subnets to route traffic through a network virtual appliance.
You can limit access to Azure resources to specific subnets with a virtual network service endpoint. You can create multiple subnets, and enable a service endpoint for some subnets, but not others.
Considerations for virtual networks

When planning to implement virtual networks, you need to consider:

Ensure nonoverlapping address spaces. Make sure your VNet address space (CIDR block) doesn't overlap with your organization's other network ranges.
Is any security isolation required?
Do you need to mitigate any IP addressing limitations?
Are there connections between Azure VNets and on-premises networks?
Is there any isolation required for administrative purposes?
Are you using any Azure services that create their own VNets?
Choose the best response for each question.

Check your knowledge

1. Which of the following statements about Azure VNets is correct?

Outbound communication with the internet must be configured for each resource on the VNet.

Azure VNets enable communication between Azure resources.

Public networks like the Internet communicate by using public IP addresses. Private networks like your Azure Virtual Network use private IP addresses, which aren't routable on public networks. To support a network that exists both in Azure and on-premises, you must configure IP addressing for both types of networks.

Public IP addresses enable Internet resources to communicate with Azure resources and enable Azure resources to communicate outbound with Internet and public-facing Azure services. A public IP address in Azure is dedicated to a specific resource. A resource without a public IP assigned can communicate outbound through network address translation services, where Azure dynamically assigns an available IP address that isn't dedicated to the resource.

As an example, public resources like web servers must be accessible from the internet. You want to ensure that you plan IP addresses that support these requirements.

Use dynamic and static public IP addresses

In Azure Resource Manager, a public IP address is a resource that has its own properties. Some of the resources you can associate a public IP address resource with:

Virtual machine network interfaces
Virtual machine scale sets
Public Load Balancers
Virtual Network Gateways (VPN/ER)
NAT gateways
Application Gateways
Azure Firewall
Bastion Host
Route Server

Public IP addresses are created with an IPv4 or IPv6 address, which can be either static or dynamic.

A dynamic public IP address is an assigned address that can change over the lifespan of the Azure resource. The dynamic IP address is allocated when you create or start a virtual machine (VM). The IP address is released when you stop or delete the VM. In each Azure region, public IP addresses are assigned from a unique pool of addresses. The default allocation method is dynamic.

A static public IP address is an assigned address that is fixed over the lifespan of the Azure resource. To ensure that the IP address for the resource remains the same, set the allocation method explicitly to static. In this case, an IP address is assigned immediately. The IP address is released only when you delete the resource or change the IP allocation method to dynamic.

Choose the appropriate SKU for a public IP address

Public IP addresses are created with one of the following SKUs:

Public IP address	Standard	Basic
Allocation method	Static	For IPv4: Dynamic or Static; For IPv6: Dynamic.

Idle time-out Have an adjustable inbound originated flow idle time out of 4-30 minutes, with a default of 4 minutes, and fixed outbound originated flow idle time out of 4 minutes. Have an adjustable inbound originated flow idle time out of 4-30 minutes, with a default of 4 minutes, and fixed outbound originated flow idle time out of 4 minutes.
Security Secure by default model and be closed to inbound traffic when used as a frontend. Allow traffic with network security group (NSG) is required (for example, on the NIC of a virtual machine with a Standard SKU Public IP attached). Open by default. Network security groups are recommended but optional for restricting inbound or outbound traffic
Availability zones Supported. Standard IPs can be nonzonal, zonal, or zone-redundant. Zone redundant IPs can only be created in regions where there are three availability zones. Not supported.
Routing preference Supported to enable more granular control of how traffic is routed between Azure and the Internet. Not supported.
Global tier Supported via cross-region load balancers. Not supported.
Choose the best response for each question.

Check your knowledge

1. Which of the following statements about Azure Public IP addresses is correct?

Standard Public IPs are Dynamically allocated.

Basic Public IPs are supported in Availability Zones.

Public IP addresses allow Internet resources to communicate inbound to Azure resources.
2. What is the difference between a static public IP address and a dynamic public IP address?

A dynamic IP address remains the same over the lifespan of the resource.

A static IP address can use an IPv4 address only.

A static IP address remains the same over the lifespan of the resource.
Next unit: Exercise: Design and implement a virtual network in Azure
Need help? See our troubleshooting guide or provide specific feedback by reporting an issue.

Design name resolution for your virtual network
Azure provides both public and private DNS services.

Public DNS services
Azure public DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers. Each DNS query is directed to the closest available DNS server. Azure DNS

provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without needing to add a custom DNS solution.

Configuration considerations
The name of the DNS zone must be unique within the resource group, and the zone must not exist already.
The same zone name can be reused in a different resource group or a different Azure subscription.
Where multiple zones share the same name, each instance is assigned different name server addresses.
The root/parent zone is registered at the registrar and pointed to Azure NS name servers.
Delegate DNS Domains
Azure DNS allows you to host a DNS zone and manage the DNS records for a domain in Azure. In order for DNS queries for a domain to reach Azure DNS, the domain has to be delegated to Azure DNS from the parent domain. Keep in mind Azure DNS isn't the domain registrar.

To delegate your domain to Azure DNS, you first need to know the name server names for your zone. Each time a DNS zone is created Azure DNS allocates name servers from a pool. Once the Name Servers are assigned, Azure DNS automatically creates authoritative NS records in your zone.

Once the DNS zone is created, and you have the name servers, you need to update the parent domain. Each registrar has their own DNS management tools to change the name server records for a domain. In the registrar’s DNS management page, edit the NS records and replace the NS records with the ones Azure DNS created.

Note

When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS. You should always use all four name server names, regardless of the name of your domain.

Child Domains
If you want to set up a separate child zone, you can delegate a subdomain in Azure DNS. For example, after configuring contoso.com in Azure DNS, you could configure a separate child zone for partners.contoso.com.

Setting up a subdomain follows the same process as typical delegation. The only difference is that NS records must be created in the parent zone contoso.com in Azure DNS, rather than in the domain registrar.

Note

The parent and child zones can be in the same or different resource group.

Private DNS services

Private DNS services 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. By using private DNS zones, you can use your own custom domain name instead of the Azure-provided names during deployment. Using a custom domain name helps you tailor your virtual network architecture to best suit your organization's needs. It provides a naming resolution for virtual machines (VMs) within a virtual network and connected virtual networks.

Considerations

Removes the need for creating custom DNS solutions.

Hosts your custom DNS records, including hostname records.

Provides hostname resolution between virtual networks.

Private DNS zones can be shared between virtual networks. This capability simplifies cross-network and service-discovery scenarios, such as virtual network peering.

The Azure DNS private zones feature is available in all Azure regions in the Azure public cloud.

Azure Private DNS Zones

Private DNS zones in Azure are available for internal resources only. They're global in scope, so you can access them from any region, any subscription, any VNet, and any tenant. If you have permission to read the zone, you can use it for name resolution. Private DNS zones are highly resilient, being replicated to regions all throughout the world. They aren't available to resources on the internet.

For scenarios which require more flexibility than internal DNS allows, you can create your own private DNS zones. These zones enable you to:

Configure a specific DNS name for a zone.

Create records manually when necessary.

Resolve names and IP addresses across different zones.

Resolve names and IP addresses across different VNets.

Tip

Learn more about Azure DNS in the Host your domain on Azure DNS module.

Enable cross-virtual network connectivity with peering

Organizations with large scale operations create connections between different parts of their virtual network infrastructure. Virtual network peering enables you to seamlessly connect separate VNets with optimal network performance, whether they are in the same Azure region (VNet peering) or in different regions (Global VNet peering).

Network traffic between peered virtual networks is private. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure, and no public Internet, gateways, or encryption is required in the communication between the virtual networks.

Virtual network peering enables you to seamlessly connect two Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes. There are two types of VNet peering.

Regional VNet peering connects Azure virtual networks in the same region.
Global VNet peering connects Azure virtual networks in different regions. The peered virtual networks can exist in any Azure public cloud region or China cloud regions, but not in Government cloud regions. You can only peer virtual networks in the same region in Azure Government cloud regions.
Diagram with VNet1 in Region 1, and VNet2 and VNet3 in Region 2. VNet2 and VNet3 are connected with regional VNet peering. VNet1 and VNet2 are connected with a global VNet peering.

Benefits of virtual network peering
The benefits of using virtual network peering, whether local or global, include:

A low-latency, high-bandwidth connection between resources in different virtual networks.
The ability to apply network security groups in either virtual network to block access to other virtual networks or subnets.
The ability to transfer data between virtual networks across Azure subscriptions, Microsoft Entra tenants, deployment models, and Azure regions.
The ability to peer virtual networks created through the Azure Resource Manager.
The ability to peer a virtual network created through Resource Manager to one created through the classic deployment model.
No downtime to resources in either virtual network is required when creating the peering, or after the peering is created.
Configure VNet Peering
Here are the steps to configure VNet peering. Notice you need two virtual networks. To test the peering, you need a virtual machine in each network. Initially, the VMs won't be able to communicate, but after peering the communication works.

Create two virtual networks.
Peer the virtual networks.
Create virtual machines in each virtual network.
Test the communication between the virtual machines.
Note

When you add a peering on one virtual network, the second virtual network configuration is automatically added.

Gateway Transit and Connectivity

You can configure a VPN gateway in the peered virtual network as a gateway transit point. In this case, a peered virtual network uses the remote gateway to gain access to other resources. A virtual network can have only one gateway. Gateway transit is supported for both VNet Peering and Global VNet Peering.

Gateway Transit allows the virtual network to communicate to resources outside the peering. For example, the subnet gateway could:

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.
In these scenarios, gateway transit allows peered virtual networks to share the gateway and get access to resources. This means you don't need to deploy a VPN gateway in the peer virtual network.

Screenshot of virtual network peering configuration page.

Note

Network security groups can be applied in either virtual network to block access to other virtual networks or subnets.

Implement virtual network traffic routing
Azure automatically creates a route table for each subnet within an Azure virtual network. The route table has the default system routes and any user defined routes you require. and adds system default routes to the table.

System routes
Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create or remove system routes, but you can override some system routes with custom routes. Azure creates default system routes for each subnet, and adds other optional default routes to specific subnets, or every subnet, when you use specific Azure capabilities.

Default system routes
Whenever a virtual network is created, Azure automatically creates the following default system routes for each subnet within the virtual network. Each system route contains an address prefix and next hop type.

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None

Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

In routing terms, a hop is a waypoint on the overall route. Therefore, the next hop is the next waypoint that the traffic is directed to on its journey to its ultimate destination. The next hop types are defined as follows:

Virtual network: Routes traffic between address ranges within the address space of a virtual network. Azure creates a route with an address prefix that corresponds to each address range defined within the address space of a virtual network. Azure automatically routes traffic between subnets using the routes created for each address range.

Internet: Routes traffic specified by the address prefix to the Internet. The system default route specifies the 0.0.0.0/0 address prefix. Azure routes traffic for any address not specified by an address range within a virtual network to the Internet, unless the destination address is for an Azure service. Azure routes any traffic destined for its service directly to the service over the backbone network, rather than routing the traffic to the Internet. You can override Azure's default system route for the 0.0.0.0/0 address prefix with a custom route.

None: Traffic routed to the None next hop type is dropped, rather than routed outside the subnet.

Screenshot of the next hop drop-down.

Optional default system routes

Azure adds default system routes for any Azure capabilities that you enable. Depending on the capability, Azure adds optional default routes to either specific subnets within the virtual network, or to all subnets within a virtual network.

Source	Address prefixes	Next hop type	Subnet within virtual network that route is added to
Default	Unique to the virtual network, for example: 10.1.0.0/16	Virtual network peering	All
Virtual network gateway	Prefixes advertised from on-premises via BGP, or configured in the local network gateway.		All
Default	Multiple	VirtualNetworkServiceEndpoint	Only the subnet a service endpoint is enabled for.

Virtual network (VNet) peering: When you create a virtual network peering between two virtual networks, a route is added for each address range within the address space of each virtual network.

Virtual network gateway: When you add a virtual network gateway to a virtual network, Azure adds one or more routes with Virtual network gateway as the next hop type. The source is listed as virtual network gateway because the gateway adds the routes to the subnet.

VirtualNetworkServiceEndpoint: Azure adds the public IP addresses for certain services to the route table when you enable a service endpoint to the service. Service endpoints are enabled for individual subnets within a virtual network, so the route is only added to the route table of a subnet a service endpoint is enabled for. The public IP addresses of Azure services change periodically, and Azure manages the updates to the routing tables when necessary.

User defined routes

You can override the default routes that Azure creates with user-defined routes (UDR). This technique can be useful when you want to ensure that traffic between two subnets passes through a firewall appliance. These custom routes override Azure's default system routes. In Azure, each subnet can have zero or one associated route table. When you create a route table and associate it to a subnet, the routes within it are combined with, or override, the default routes Azure adds to a subnet.

You can specify the following next hop types when creating a user-defined route:

Virtual appliance: A virtual appliance is a virtual machine that typically runs a network application, such as a firewall. When you create a route with the virtual appliance hop type, you also specify a next hop IP address.

Virtual network gateway: Specify when you want traffic destined for specific address prefixes routed to a virtual network gateway. The virtual network gateway must be created with type VPN.

None: Specify when you want to drop traffic to an address prefix, rather than forwarding the traffic to a destination.

Virtual network: Specify when you want to override the default routing within a virtual network.

Internet: Specify when you want to explicitly route traffic destined to an address prefix to the Internet.

Consider Azure Route Server

Azure Route Server simplifies dynamic routing between your network virtual appliance (NVA) and your virtual network. Azure Route Server is a fully managed service and is configured with high availability. Azure Route Server simplifies configuration, management, and deployment of your NVA in your virtual network.

You no longer need to manually update the routing table on your NVA whenever your virtual network addresses are updated.

You no longer need to update user defined routes manually whenever your NVA announces new routes or withdraws old ones.

You can peer multiple instances of your NVA with Azure Route Server.

The interface between NVA and Azure Route Server is based on a common standard protocol. As long as your NVA supports BGP, you can peer it with Azure Route Server.

You can deploy Azure Route Server in any of your new or existing virtual network.

Troubleshoot with effective routes

Imagine your attempts to connect to a specific virtual machine (VM) in your Azure virtual network consistently fail. You can diagnose a routing problem by viewing the effective for a virtual machine network interface. You can view the effective routes for each network interface by using the Azure portal.

Configure internet access with Azure Virtual NAT

Globally, IPv4 address ranges are in short supply, and can be an expensive way to grant access to Internet resources. Azure Network Address Translation (NAT) lets internal resources on a private network to share routable IPv4 addresses. Rather than purchasing an IPv4 address for each resource that requires internet access, you can use a NAT service to map outgoing requests from internal resources to an external IP address.

The following diagram shows outbound traffic flow from Subnet 1 through the NAT gateway to be mapped to a Public IP address or a Public IP prefix.

Diagram with NAT service providing internet connectivity for internal resources.

After NAT is configured, all UDP and TCP outbound flows from any virtual machine instance will use NAT for internet connectivity. No further configuration is necessary, and you don’t need to create any user-defined routes. NAT takes precedence over other outbound scenarios and replaces the default Internet destination of a subnet.

NAT scales automatically to support dynamic workloads. NAT can support up to 16 public IP addresses. By using port network address translation (PNAT or PAT), NAT provides up to 64,000 concurrent flows for UDP and TCP. NAT is compatible with the following standard SKU resources:

Load balancer
Public IP address
Public IP prefix
Limitations of NAT
Basic resources (for example basic load balancer) and any products derived from them aren't compatible with NAT. Basic resources must be placed on a subnet not configured with NAT.
Only the IPv4 address family is supported. NAT doesn't interact with IPv6 address family.
NAT can't span multiple virtual networks.
IP fragmentation isn't supported.