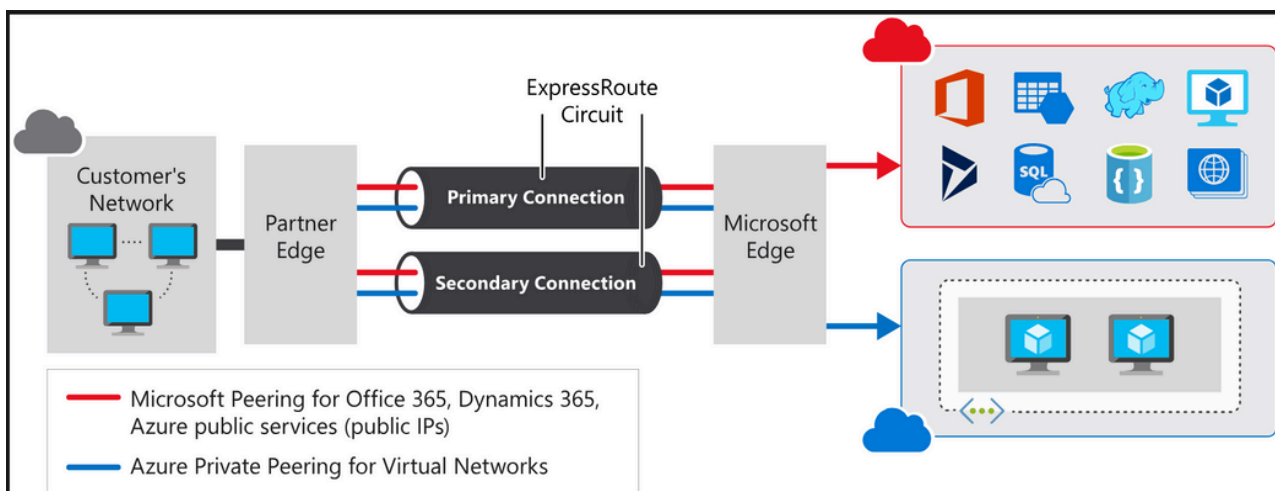


# How Azure ExpressRoute Works

Azure ExpressRoute provides a dedicated, private network connection between your on-premises infrastructure and Microsoft Azure datacenters. Instead of traversing the public internet, traffic flows through a connectivity provider's network, offering more reliable and predictable performance, higher bandwidth, lower latency, and enhanced security.

At a high level, the process involves:

1. **Establishing a connection with a connectivity provider:** You'll work with a provider that has a physical connection to Microsoft's network at an ExpressRoute location.
2. **Creating an ExpressRoute circuit:** This is a logical connection that represents the dedicated path between your network and Azure. You'll specify the bandwidth and peering types (Private and/or Microsoft).
3. **Configuring routing:** Once the circuit is provisioned, you'll configure routing to direct traffic between your on-premises network and your Azure virtual networks (for Private Peering) or Azure services (for Microsoft Peering). This typically involves Border Gateway Protocol (BGP) peering with Microsoft's routers.



## Prerequisites for ExpressRoute

Before deploying Azure ExpressRoute, several prerequisites need to be in place:

- **Azure Subscription:** You need an active Azure subscription.
- **Connectivity Provider:** Engage with an Azure ExpressRoute connectivity provider.
- **Network Infrastructure:** Ensure your on-premises network is capable of connecting to the chosen ExpressRoute location. This includes having compatible routing equipment that supports BGP.
- **ExpressRoute Location:** Select an ExpressRoute location that is geographically convenient and supported by your chosen provider.
- **IP Addressing:** Plan your private and public IP address ranges for the ExpressRoute interfaces.
- **Virtual Network Gateway:** For Private Peering, you'll need an ExpressRoute virtual network gateway deployed in your Azure virtual network.
- **Authorization Key and Peer ASN:** You'll receive an authorization key and need to provide your Autonomous System Number (ASN) to your connectivity provider.

## ExpressRoute Locations (Peering or Meet-Me Locations)

ExpressRoute locations are crucial as they are the physical points of interconnection between your connectivity provider's network and the Microsoft Enterprise Edge (MSEE) routers. These globally distributed facilities enable you to establish connectivity to Microsoft's global network.

### Key Considerations for ExpressRoute Locations:

- **Geographical Proximity:** Choose a location close to your on-premises infrastructure to minimize latency.
- **Connectivity Provider Availability:** Ensure your preferred connectivity provider has a presence at the desired location.

- **Service Availability:** All Azure regions within a geopolitical region are accessible if you connect to at least one ExpressRoute location within that region.
- **Global Connectivity:** The standard ExpressRoute SKU offers connectivity within a single geopolitical region. The **ExpressRoute Premium Add-on** is required for global connectivity across geopolitical boundaries.

## Available Connectivity Providers for Azure ExpressRoute

Azure ExpressRoute offers flexibility in how you connect to Microsoft's network through various types of connectivity providers:

- **ExpressRoute Connectivity Providers:** These are telecommunication operators or network service providers that offer direct Layer 2 or Layer 3 connections between your on-premises infrastructure and Azure ExpressRoute locations. They manage the physical connection and routing.
- **Connectivity Through Exchange Providers:** These providers operate large, carrier-neutral colocation facilities. You can connect to their exchange points, and they will facilitate the connection to the Microsoft Enterprise Edge routers within the same facility. This model often provides access to multiple connectivity providers.
- **Connectivity Through Satellite Operators:** For organizations in remote locations where terrestrial connectivity is limited, satellite operators can provide ExpressRoute connections.

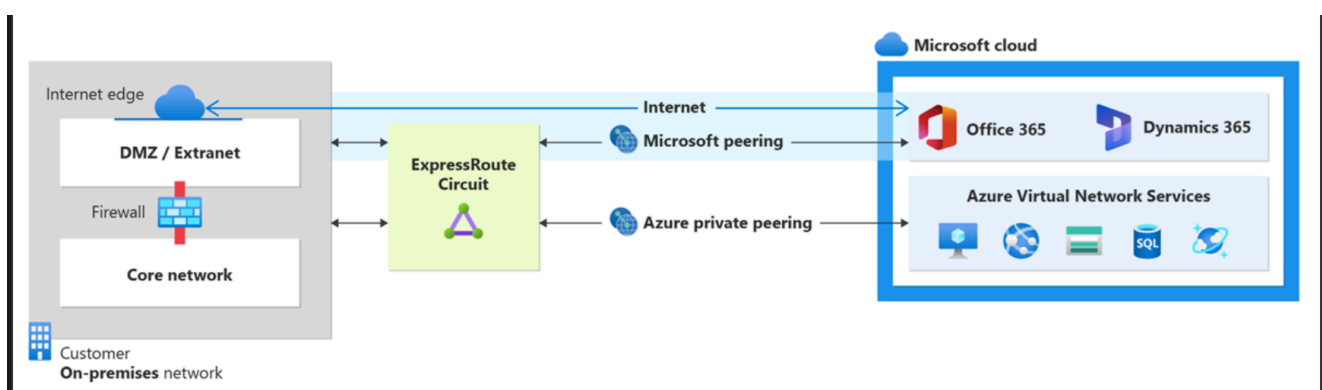
## Creating an ExpressRoute Circuit and Peering

The process of creating an ExpressRoute circuit involves the following steps:

1. **Using the Azure portal, PowerShell, or Azure CLI:** You'll create an ExpressRoute circuit resource within your Azure subscription.
2. **Specifying configuration details:** This includes the location, bandwidth, billing model, and SKU.
3. **Receiving the Service Key:** Once the circuit is created, you'll receive a unique service key. You'll share this key with your chosen connectivity provider to establish the physical connection.
4. **Provider Provisioning:** The connectivity provider will provision the connection on their end and update the circuit status in Azure to "Provisioned."

After the provider status is "Provisioned," you can configure the **peerings**:

- **Private Peering:** Enables you to connect your on-premises network to Azure Virtual Networks (VNETs). You'll configure private IP addresses and establish BGP sessions with Microsoft's private peering routers. This allows seamless connectivity to your IaaS and PaaS resources within your VNETs.
- **Microsoft Peering:** Allows you to connect to Microsoft SaaS/PaaS services like Microsoft 365, Dynamics 365, and Azure public services (e.g., Azure Storage, Azure SQL Database). You'll need to use public IP addresses for this peering and configure BGP sessions with Microsoft's Microsoft peering routers.



## Considerations for Choosing an Azure ExpressRoute Peering Location

Selecting the right ExpressRoute peering location is crucial for performance and cost optimization. Consider the following:

- **Proximity to your on-premises data centers:** Lower latency and better performance can be achieved by choosing a location geographically close to your infrastructure.
- **Availability of your chosen connectivity provider:** Ensure your preferred provider supports the location.

- **Azure region access:** Remember that connecting to one ExpressRoute location within a geopolitical region grants access to all Azure regions within that region.
- **Disaster recovery requirements:** Consider pairing ExpressRoute circuits in different locations for enhanced resilience.
- **Cost implications:** Different locations might have varying costs associated with connectivity.

## Connecting a Virtual Network to an ExpressRoute Circuit

To connect a virtual network to an ExpressRoute circuit (for Private Peering), you need to create an **ExpressRoute virtual network gateway** within your VNet. This gateway serves as the connection point between the VNet and the ExpressRoute circuit.

The steps involved are:

**Create a Virtual Network Gateway:** Choose the gateway type as "ExpressRoute." Ensure the gateway subnet has sufficient address space.

To connect your Azure virtual network and your on-premises network via ExpressRoute, you must create a virtual network gateway first. A virtual network gateway serves two purposes: to exchange IP routes between the networks and to route network traffic.

When you create a virtual network gateway, you need to specify several settings. One of the required settings, '-GatewayType', specifies whether the gateway is used for ExpressRoute, or VPN traffic. The two gateway types are:

- **VPN** - To send encrypted traffic across the public Internet, you use the gateway type 'VPN'. This is also referred to as a VPN gateway. Site-to-Site, Point-to-Site, and VNet-to-VNet connections all use a VPN gateway.
- **ExpressRoute** - To send network traffic on a private connection, you use the gateway type 'ExpressRoute'. This is also referred to as an ExpressRoute gateway and is the type of gateway used when configuring ExpressRoute.

Each virtual network can have only one virtual network gateway per gateway type. For example, you can have one virtual network gateway that uses -GatewayType VPN, and one that uses -GatewayType ExpressRoute.

In this exercise, you will

### - Task 1: Create the VNet and gateway subnet

On any Azure Portal page, in **Search resources, services and docs**, enter virtual network, and then select **Virtual networks** from the results.

→ On the Virtual networks page, select **+Create**.

→ On the Create virtual networks pane, on the **Basics** tab, use the information in the following table to create the VNet:

<b>Setting</b>	<b>Value</b>	
-----	-----	
Virtual Network Name	CoreServicesVNet	
Resource Group	ContosoResourceGroup	
Location	East US	

Select **Next : IP addresses**.

On the **IP Addresses** tab, in **IPv4 address space**, enter 10.20.0.0/16, and then select **+ Add subnet**.

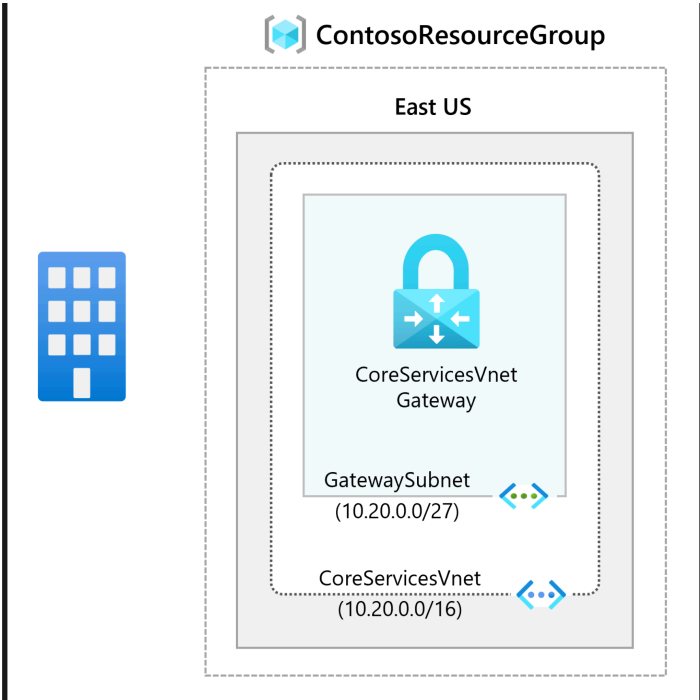
In the Add subnet pane, use the information in the following table to create the subnet:

Setting	Value
Subnet purpose	Virtual Network Gateway
Gateway Subnet address space	10.20.0.0/27

Note that the subnet name will be automatically populated. And then select **Add**.

→ On the Create virtual network page, select **Review + Create**.

→ Confirm that the VNet passes the validation and then select **Create**.



# Create virtual network ...

- Basics
- Security
- IP addresses
- 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.](#)

## Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Azure subscription 1

Resource group \*

ContosoResourceGroup

[Create new](#)

## Instance details

Virtual network name \*

CoreServicesVNet

Region \* ⓘ

(US) East US

[Deploy to an Azure Extended Zone](#)

Home > Virtual networks >

Create virtual network

Basics

Security

IP addresses

Tags

Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, the resource is assigned an IP address from the subnet. [Learn more](#)

+ Add a subnet

10.20.0.0/16

10.20.0.0

/16

10.20.0.0 - 10.20.255.255

65,536 addresses

Delete address

Subnets	IP address range	Size	NAT gateway
GatewaySubnet	10.20.1.0 - 10.20.1.31	/27 (32 addresses)	-

Add IPv4 address space

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose

Virtual Network Gateway

Name \*

GatewaySubnet

IPv4

Include an IPv4 address space

10.20.0.0/16

10.20.0.0 - 10.20.255.255

Starting address \*

10.20.1.0

Size

/27 (32 addresses)

Subnet address range

10.20.1.0 - 10.20.1.31

IPv6

Include an IPv6 address space

This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access)

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway

None

Create new

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)

Network security group

None

Create new

Route table

None

Service Endpoints

Create service endpoint policies to allow traffic to specific Azure resources from your virtual network over service endpoints. [Learn more](#)

Services

Remove service endpoint

## - Task 2: Create the virtual network gateway

→ On any Azure Portal page, in **Search resources, services and docs (G+)**, enter virtual network gateway, and then select **Virtual network gateways** from the results.

→ On the Virtual network gateways page, select **+Create**.

→ On the **Create virtual network gateway** page, use the information in the following table to create the gateway:

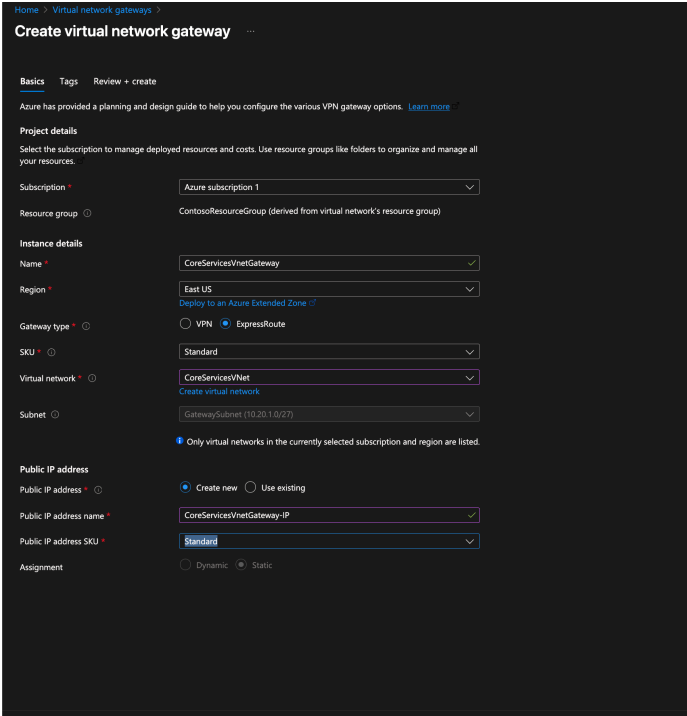
Setting	Value
Project details	
Resource Group	ContosoResourceGroup
Instance details	
Name	CoreServicesVnetGateway
Region	East US
Gateway type	ExpressRoute
SKU	Standard
Virtual network	CoreServicesVNet

Public IP address		
Public IP address	Create new	
Public IP address name	CoreServicesVnetGateway-IP	
Assignment	Not configurable	

Select **Review + Create**.

Confirm that the Gateway configuration passes validation and then select **Create**.

When the deployment is complete, select **Go to Resource**.



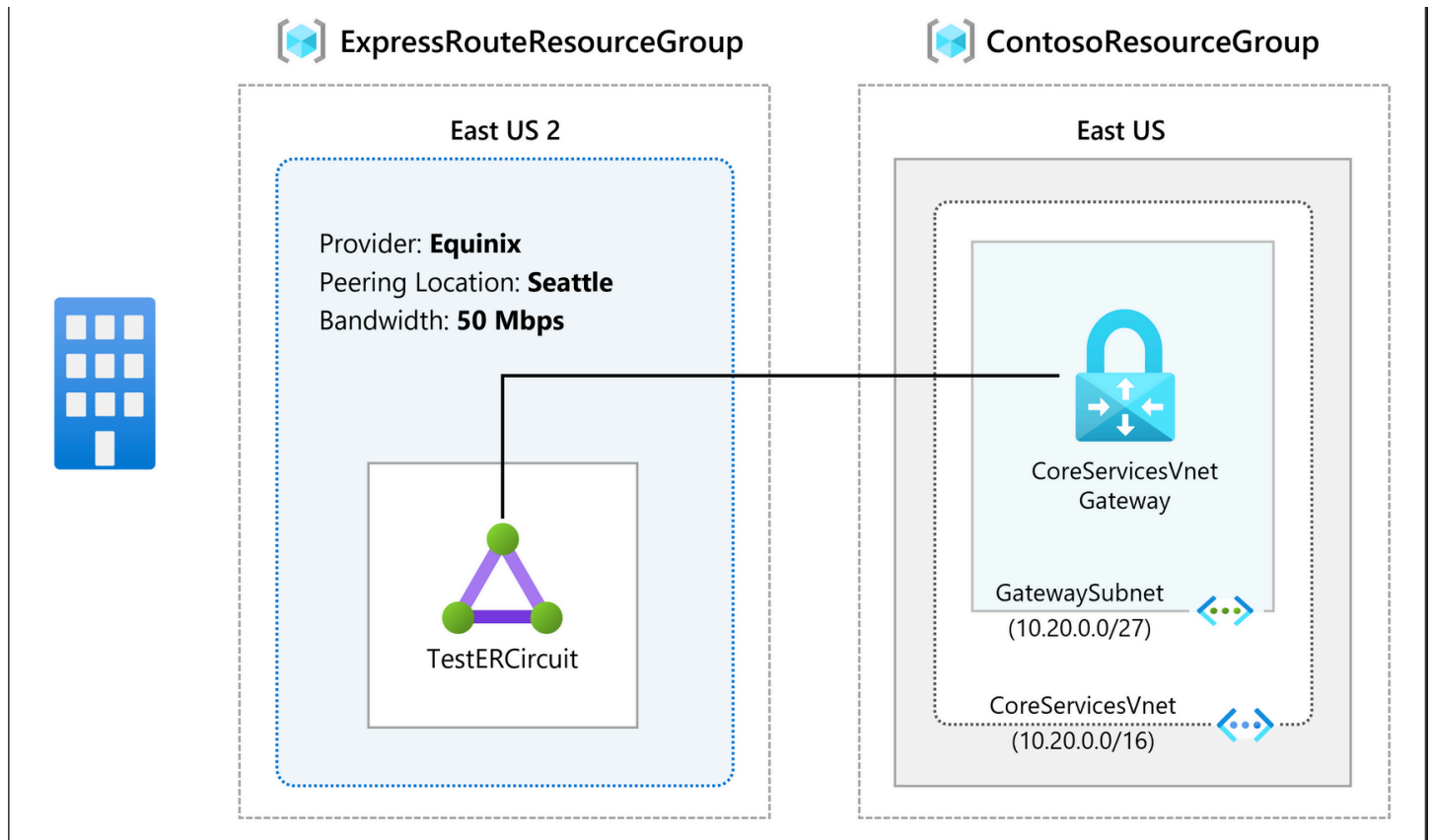
**Create a Connection:** Link the ExpressRoute gateway to your ExpressRoute circuit, providing the resource ID of the circuit and an authorization key (if the circuit is in a different subscription).

Once the connection is established, traffic can flow between your on-premises network and the virtual network over the private ExpressRoute connection.

**In this exercise, you will:**

**## Task 1: Create and provision an ExpressRoute circuit**

**>Important:** Your ExpressRoute circuit is billed from the moment a service key is issued. Ensure that you perform this operation when the connectivity provider is ready to provision the circuit.



→ On the Azure portal menu, select **+++ Create a resource**. Select **Networking**, and then select **ExpressRoute**, as shown in the following image. If ExpressRoute does not appear in the list, use **Search the marketplace** to search for it:

→ On the **Create ExpressRoute** page, provide the **Resource Group** as ExpressRouteResourceGroup. Then select **Standard Resiliency** for **Resiliency**

For **Circuit Details**, make sure that you specify the correct Region (**East US 2**), Circuit Name (**TestERCircuit**), Peering location (**Seattle**), Provider (**Equinix**), Bandwidth (**50Mbps**), SKU tier (**Standard**) and data metering billing model (**Metered**).

Select **Review + Create**.



Home > ExpressRoute circuits >

## Create ExpressRoute

Subscription \* ⓘ Azure subscription 1

Resource group \* ⓘ (New) ExpressRouteResourceGroup  
[Create new](#)

Resiliency

☐ Maximum Resiliency (Recommended): Resiliency across two or more distinct edge locations each with redundant physical links  
☐ High Resiliency: Metro model offering resiliency across distinct edge locations each with single physical link  
☒ Standard Resiliency: Physical link redundancy within one edge location only

**i** Does not protect against location-wide outages. Suitable for non-critical / non-production workloads.

**Circuit Details**

Region \* East US

Circuit name \* ⓘ TestERCircuit ✓

Port type ⓘ

☒ Provider  
☐ Direct

Peering location \* ⓘ Seattle

Provider \* ⓘ Equinix

Bandwidth \* ⓘ 50Mbps

SKU ⓘ

☐ Local  
☒ Standard  
☐ Premium

Billing model ⓘ

☒ Metered  
☐ Unlimited

[Review + create](#)
[Previous](#)
[Next : Monitoring >](#)
[Download a template for automation](#)

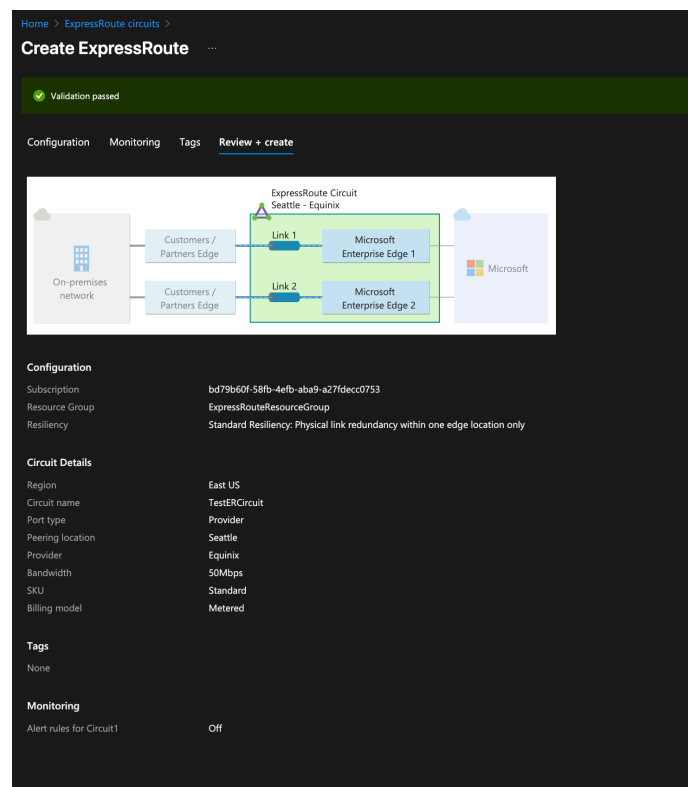
Confirm that the ExpressRoute configuration passes validation and then select **\*\*Create\*\***.

+ Port type determines if you are connecting to a service provider or directly into Microsoft's global network at a peering location.

+ Create new or import from classic determines if a new circuit is being created or if you are migrating a classic circuit to Azure Resource Manager.

+ Provider is the internet service provider who you will be requesting your service from.

+ Peering Location is the physical location where you are peering with Microsoft.



[!Important]

The Peering Location indicates the [physical location](<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations>) where you are peering with Microsoft. This is not linked to "Location" property, which refers to the geography where the Azure Network Resource Provider is located. While they are not related, it is a good practice to choose a Network Resource Provider geographically close to the Peering Location of the circuit.

+ **SKU** determines whether an ExpressRoute local, ExpressRoute standard, or an ExpressRoute premium add-on is enabled. You can specify **Local** to get the local SKU, **Standard** to get the standard SKU or **Premium** for the premium add-on. You can change the SKU to enable the premium add-on.

→**Important**: You cannot change the SKU from Standard/Premium to Local.

+ **Billing model** determines the billing type. You can specify **Metered** for a metered data plan and **Unlimited** for an unlimited data plan. You can change the billing type from **Metered** to **Unlimited**.

[!Important] You cannot change the type from Unlimited to Metered.

+ **Allow classic operation** will allow classic virtual networks to be link to the circuit.

## ## Task 2: Retrieve your Service key

You can view all the circuits that you created by selecting **All services >> Networking >> ExpressRoute circuits**.

All ExpressRoute circuits created in the subscription will appear here.

The circuit page displays the properties of the circuit. The service key appears in the service key field. Your service provider will need the Service Key to complete the provisioning process. The service key is specific to your circuit. **You must send the service key to your connectivity provider for provisioning.**

On this page, **Provider status** gives you the current state of provisioning on the service-provider side. **Circuit status** provides you the state on the Microsoft side.

When you create a new ExpressRoute circuit, the circuit is in the following state:

- + Provider status: Not provisioned
- + Circuit status: Enabled
- + The circuit changes to the following state when the connectivity provider is currently enabling it for you:
  - + Provider status: Provisioning
  - + Circuit status: Enabled
- + To use the ExpressRoute circuit, it must be in the following state:
  - + Provider status: Provisioned
  - + Circuit status: Enabled
- + You should periodically check the provisioning status and the state of the circuit status.

Congratulations! You have created an ExpressRoute circuit and located the Service key, which you would need to complete the provisioning of the circuit.

"In this lab environment, while we successfully created the ExpressRoute circuit and obtained the crucial Service key, the circuit status remains in a pending state. This is a standard expectation when working through the initial setup without engaging a live connectivity provider. The Service key generated for this circuit is the vital piece of information that would now need to be shared with our chosen ExpressRoute provider, in this case, Equinix. Once Equinix receives the Service key, they would then proceed to provision the physical and logical connections on their end, linking our network infrastructure to the Microsoft Enterprise Edge routers at the designated peering location. After Equinix completes their provisioning process, the 'Provider status' of our ExpressRoute circuit in the Azure portal would transition from 'Not provisioned' to 'Provisioned,' signifying that the dedicated connectivity has been successfully established and is ready for peering configuration."

Home > **TestERCircuit** ExpressRoute circuit

Search Delete Refresh

**Overview**

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
- Monitoring
- Automation
- Help

Initiate the provisioning process with your service provider.

**Essentials** [JSON View](#)

Resource group (move) : [ExpressRouteResourceGroup](#)

Provider : Equinix

Circuit status : Enabled

Provider status : Not provisioned

Location : East US

Peering location : Seattle

Subscription (move) : [Azure subscription 1](#)

Bandwidth : 50 Mbps

Subscription ID : bd79b60f-58fb-4efb-aba9-a27fdecc0753

Service key : 5f7a4-...

Tags (edit) : [Add tags](#)

**Health check**  
Perform a quick health check to detect possible expressroute issues  
[Go to Resource health](#)

**Advisor Recommendations**  
Check Critical, Warning, and Informational Recommendations  
[Go to Advisor](#)

**Documentation**  
View guidance on helpful topics related to ExpressRoute  
[View documentation](#)

**Peerings**

Type	Status	Primary subnet	Secondary subnet	Last modified by
<a href="#">Azure private</a>	Not provisioned	-	-	-
<a href="#">Azure public</a>	Not provisioned	-	-	-
<a href="#">Microsoft</a>	Not provisioned	-	-	-

**Global Reach**

ExpressRoute Global Reach allows you to link your ExpressRoute circuits together to make a private network between your on-premises networks. With Global Reach, your branch offices can directly exchange data with each other through your ExpressRoute circuits and via Microsoft's global network.  
[Learn more](#)

Global Reach name	ExpressRoute Circuit name	IPv4 Subnet	IPv6 Subnet
<a href="#">Add Global Reach</a>	<a href="#">Save</a>		

**ExpressRoute Traffic Collector**

ExpressRoute Traffic Collector provides access to sampled flow logs, enabling better visibility into your ExpressRoute usage.  
[Learn more](#)

Name	Resource Group	Location	Subscription	Status
<a href="#">Configure ExpressRoute Traffic Collectors</a>				

## ## Task 3: Deprovisioning an ExpressRoute circuit

If the ExpressRoute circuit service provider provisioning state is **Provisioning** or **Provisioned**, you must work with your service provider to deprovision the circuit on their side. Microsoft can continue to reserve resources and bill you until the service provider completes deprovisioning the circuit and notifies us.

→**Note**: You must unlink all virtual networks from the ExpressRoute circuit before deprovisioning. If this operation fails, check whether any virtual networks are linked to the circuit. If the service provider has deprovisioned the circuit (the service provider provisioning state is set to Not provisioned), you can delete the circuit. This stops billing for the circuit.

### ## Clean up resources

You can delete your ExpressRoute circuit by selecting the **Delete** icon. Ensure the provider status is Not provisioned before proceeding

## Choosing Between an ExpressRoute Provider Model and ExpressRoute Direct

### Azure offers two primary models for ExpressRoute connectivity:

"With the ExpressRoute circuit provisioned by a provider like Equinix, the real power of this dedicated connection unlocks. Imagine a secure, high-speed pipeline directly linking your on-premises data center to the vast resources of Azure. This isn't just about faster data transfers; it's about enabling seamless hybrid cloud scenarios, running mission-critical applications with consistent performance, and extending your network with enterprise-grade reliability. The next exciting step involves configuring the peerings – Private Peering to connect your virtual networks and Microsoft Peering to access Azure's rich ecosystem of services, including Microsoft 365. This is where you truly tailor the ExpressRoute connection to meet your specific cloud strategy and workload requirements, paving the way for innovation and agility."

Feature	ExpressRoute Provider Model	ExpressRoute Direct
<b>Connectivity</b>	Connect through a third-party connectivity provider.	Connect directly to Microsoft's global network at peering locations.
<b>Port Speed Options</b>	Typically up to 10 Gbps, depending on the provider.	10 Gbps or 100 Gbps dedicated ports.
<b>Management</b>	The provider manages the physical connection. You manage the logical circuit and peerings.	You manage the physical cross-connections to Microsoft's routers. Microsoft manages the routing on their end.
<b>Redundancy</b>	Provider-dependent; Microsoft offers options for circuit redundancy.	Built-in redundancy with dual ports per ExpressRoute Direct resource.
<b>Use Cases</b>	Organizations with standard bandwidth requirements, leveraging existing provider relationships.	Organizations requiring high bandwidth, direct control over physical connections, and support for features like MACsec for enhanced security. Suitable for large enterprises and scenarios with stringent compliance requirements.
<b>Cost</b>	Typically lower upfront costs but recurring provider charges.	Higher upfront costs for port fees but potentially lower per-unit bandwidth costs at scale.
<b>Supported Peerings</b>	Private and Microsoft Peering.	Private, Microsoft, and Azure Global Reach are supported.

## Azure ExpressRoute SKU and Features

Feature	Standard SKU	Premium SKU
Global Connectivity	Not supported. Connectivity is limited to a single geopolitical region.	Supported. Enables connectivity across geopolitical regions.
Number of VNets	Limited number of virtual networks can be connected per ExpressRoute circuit.	Higher limits on the number of virtual networks that can be connected per ExpressRoute circuit.
Number of Routes	Limited number of routes advertised over BGP.	Higher limits on the number of routes advertised over BGP.
Microsoft Peering Access to Global Services	Access to services within the same geopolitical region.	Access to Microsoft's global services (e.g., Microsoft 365 services globally).
Cost	Generally lower cost.	Higher cost due to the added features and increased limits.
Use Cases	Organizations with regional connectivity needs and standard scale requirements.	Organizations with global presence, large-scale deployments, and requirements for connecting to Microsoft's global SaaS offerings.

**Azure ExpressRoute Circuit Configuration Details**

Configuration Element	Description
<b>Circuit Name</b>	A user-friendly name to identify the ExpressRoute circuit in Azure.
<b>Location</b>	The ExpressRoute peering location where the circuit will be created.
<b>Bandwidth</b>	The provisioned capacity of the ExpressRoute circuit (e.g., 50 Mbps, 1 Gbps, 10 Gbps).
<b>Service Provider</b>	The connectivity provider you are using.
<b>Peering Location</b>	The specific meet-me location chosen for the connection.
<b>SKU</b>	The ExpressRoute SKU (Standard or Premium).
<b>Billing Model</b>	The billing option chosen (e.g., Metered Data, Unlimited Data).
<b>Provider Status</b>	Indicates the provisioning status of the circuit by the connectivity provider.
<b>Circuit Status</b>	Indicates the operational status of the ExpressRoute circuit in Azure.
<b>Peering Configuration</b>	Details for Private Peering (VNet connections, IP addressing, ASN) and Microsoft Peering (public IP prefixes, ASN, advertised communities).
<b>Authorization Key</b>	A unique key used to authorize the connection between the ExpressRoute circuit and a virtual network in a different Azure subscription.
<b>Global Reach Enabled</b>	Indicates whether Azure Global Reach is enabled for the circuit.
<b>FastPath Enabled</b>	Indicates whether ExpressRoute FastPath is enabled for the virtual network gateway connected to the circuit.
<b>Resiliency Type</b>	The resiliency configuration for the ExpressRoute circuit (Standard, High, or Maximum Resiliency).

## Features and Benefits of ExpressRoute

- **Built-in Redundancy & High Availability and Failover:** ExpressRoute is designed with redundancy at various levels. Microsoft provisions dual ports on the MSEE routers. You can also work with connectivity providers to establish redundant connections. For enhanced resiliency, consider deploying dual ExpressRoute circuits in different peering locations. Failover mechanisms can be configured at the routing level to automatically switch to a secondary path in case of a failure.
- **Connectivity to Microsoft Cloud Services:** ExpressRoute provides secure and reliable connectivity to a wide range of Microsoft cloud services, including Azure IaaS, PaaS, SaaS (Microsoft 365, Dynamics 365), and more. This enables seamless integration and hybrid cloud scenarios.
- **Resiliency:** ExpressRoute offers different resiliency options to meet varying business needs:
  - **Standard Resiliency:** Includes dual ports on the Microsoft Enterprise Edge routers.
  - **High Resiliency:** Typically involves dual ExpressRoute circuits from the same connectivity provider, potentially in the same peering location, providing path diversity.
  - **Maximum Resiliency:** Usually involves dual ExpressRoute circuits from different connectivity providers in different peering locations, offering the highest level of fault tolerance.

## ExpressRoute Circuit Resiliency Types

Resiliency Type	Description
<b>Standard Resiliency</b>	Default configuration with dual, redundant ports on the Microsoft Enterprise Edge (MSEE) routers at the peering location. This protects against failures within the MSEE devices.
<b>High Resiliency</b>	Typically involves two ExpressRoute circuits from the same connectivity provider, often in the same peering location but potentially on different physical connections. This adds redundancy in the provider's network path.
<b>Maximum Resiliency</b>	Involves two ExpressRoute circuits from <i>different</i> connectivity providers and ideally in <i>different</i> peering locations. This provides the highest level of resilience against failures in the provider's network or at a specific location.

## Primary Purpose of Microsoft ExpressRoute Peering

The primary purpose of Microsoft ExpressRoute peering is to establish **private, high-bandwidth network connections** between Azure datacenters and infrastructure on your premises or in a colocation environment. This dedicated connectivity offers benefits such as:

- **Predictable Performance:** Consistent bandwidth and lower latency compared to internet-based connections.
- **Enhanced Security:** Traffic travels over a private network, reducing exposure to the public internet.
- **Reliability:** Service level agreements (SLAs) are often offered by both Microsoft and the connectivity providers.
- **Hybrid Cloud Scenarios:** Enables seamless integration of on-premises and Azure resources.

## Azure Global Reach

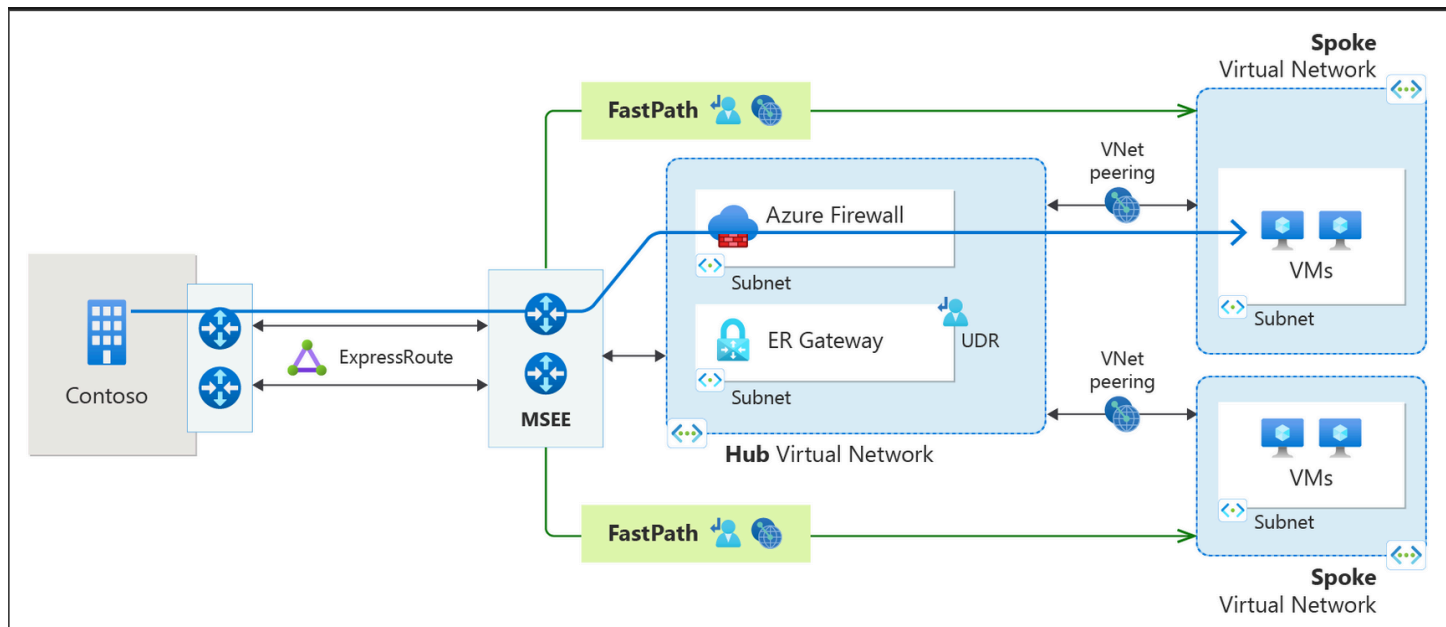
Azure Global Reach enables **direct connectivity between different geographically dispersed on-premises sites** using Microsoft's global network. It allows you to link ExpressRoute circuits together, creating a private wide area network (WAN) over the Microsoft backbone.

Think of it as similar to **VNet-to-VNet peering** or an **Azure Virtual WAN hub**, but for connecting your on-premises locations that are connected to Azure via ExpressRoute. It's designed to complement your service provider's WAN implementation and facilitate global branch office connectivity.

## Improving Data Path Performance with ExpressRoute FastPath

ExpressRoute FastPath is a feature designed to **enhance data path performance** between your on-premises network and your Azure virtual networks. Traditionally, traffic traversing an ExpressRoute connection to a VNet would always pass through the ExpressRoute virtual network gateway.





FastPath **bypasses the virtual network gateway** for supported workloads, routing network traffic directly to virtual machines within the VNet. This reduces latency and improves throughput.

#### Key aspects of FastPath:

- Available on all ExpressRoute circuits.
- Must be enabled on the ExpressRoute virtual network gateway.
- Beneficial for latency-sensitive and high-bandwidth applications.
- Supports both Private Peering and Microsoft Peering for Azure PaaS services.

### Common Configuration Issues and Troubleshooting

Common configuration issues with Azure ExpressRoute include:

- **Incorrect VLAN tagging or encapsulation.**
- **Mismatched BGP configuration parameters (ASN, IP addresses, authentication keys).**
- **Firewall rules blocking BGP or application traffic.**
- **Incorrect route advertisements.**
- **Issues with the connectivity provider's provisioning.**
- **Problems with virtual network gateway configuration.**
- **Authorization key mismatches when connecting VNets in different subscriptions.**

#### Troubleshooting ExpressRoute Connection Issues:

- **Verify the ExpressRoute circuit status in the Azure portal.**
- **Check the peering status and BGP session status.**
- **Review the configuration of your on-premises routers and the virtual network gateway.**
- **Use network monitoring tools to analyze traffic flow.**
- **Contact your connectivity provider for any physical connectivity issues.**
- **Leverage Azure Network Watcher for diagnostics and troubleshooting.**
- **Provide the service key to Microsoft support or your ExpressRoute partner for efficient issue identification.** The service key uniquely identifies your ExpressRoute circuit.

### Azure ExpressRoute vs. Virtual WAN

Feature	Azure ExpressRoute	Azure Virtual WAN
<b>Primary Purpose</b>	Dedicated, private connectivity to Azure.	Centralized network management and connectivity for hybrid and multi-cloud environments.
<b>Connectivity Model</b>	Point-to-point connection between your network and Azure via a connectivity provider or direct connection.	Hub-and-spoke architecture. Connects various sites (on-premises, branches, remote users, Azure VNets) to a central virtual hub.
<b>Connectivity Options</b>	ExpressRoute circuits.	ExpressRoute, Site-to-site VPN, Point-to-site VPN, User VPN (OpenVPN, IKEv2, SSTP).
<b>Management</b>	Managed individually per circuit.	Centrally managed through the Virtual WAN hub. Simplifies connectivity and routing management across multiple connections.
<b>Routing</b>	Requires manual configuration of BGP and route tables.	Automated routing within the virtual hub and between connected spokes. Simplifies route propagation and management.
<b>Scalability &amp; Flexibility</b>	Scalability is determined by the provisioned bandwidth of the ExpressRoute circuit.	Highly scalable and flexible for connecting numerous sites and different types of connections.
<b>Use Cases</b>	Organizations needing high-bandwidth, low-latency, and secure private connections to specific Azure resources.	Organizations with complex hybrid networking requirements, multiple branch offices, remote users, and the need for centralized management, security, and policy enforcement