Microsoft Azure ExpressRoute

Michael Washam

Guide

Microsoft

Microsoft Azure ExpressRoute

Michael Washam

Summary: Microsoft Azure ExpressRoute makes it easy to establish dedicated and private circuits between your data center and Microsoft Azure. ExpressRoute connections do not go over the public Internet and offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet. This guide explains ExpressRoute and its uses, compares provider models, and walks you through the workflow and deployment steps.

Category: Guide
Applies to: Microsoft Azure
Source: ExpressRoute Technical Overview | Source Content
E-book publication date: [July 2014]

For more titles, visit the E-Book Gallery for Microsoft Technologies.

Microsoft Azure ExpressRoute

Contents

Introduction to Microsoft Azure ExpressRoute

Microsoft Azure ExpressRoute makes it easy to establish dedicated and private circuits between your data center and Microsoft Azure. Your existing infrastructure can be located on-premises in your own data center or co-located in one of several participating provider locations. ExpressRoute allows you to extend your infrastructure to Microsoft Azure by providing private, reliable, high speed connectivity between you and the cloud.

With ExpressRoute your circuit is isolated using industry standard VLANs to allow private, secure access to resources deployed in Microsoft Azure Virtual Networks and also to provide connectivity to Microsoft Azure public services.

How does ExpressRoute help?

Network Privacy

Connectivity between your on-premises infrastructure and infrastructure hosted in Microsoft Azure is private and secure through your ExpressRoute circuit. Your traffic never traverses the public Internet when connecting to your own virtual machines or even connecting to other Microsoft Azure public services such as Storage and SQL Database through ExpressRoute.

Reduces Costs

If you have bandwidth heavy applications and workloads, Microsoft Azure ExpressRoute may reduce your bandwidth costs. Unlimited inbound traffic to Microsoft Azure is included with your circuit. If your ExpressRoute partner falls under the network service provider billing model you also have unlimited outbound traffic for the same price.

If your provider is an Exchange Provider, a significant amount of outbound traffic is included and any bandwidth between ExpressRoute linked virtual networks is unlimited and included in the cost.

Outbound traffic above and beyond the included amount in your plan will be at significantly reduced rates compared with traditional Internet Service Providers and regular Microsoft Azure bandwidth rates.
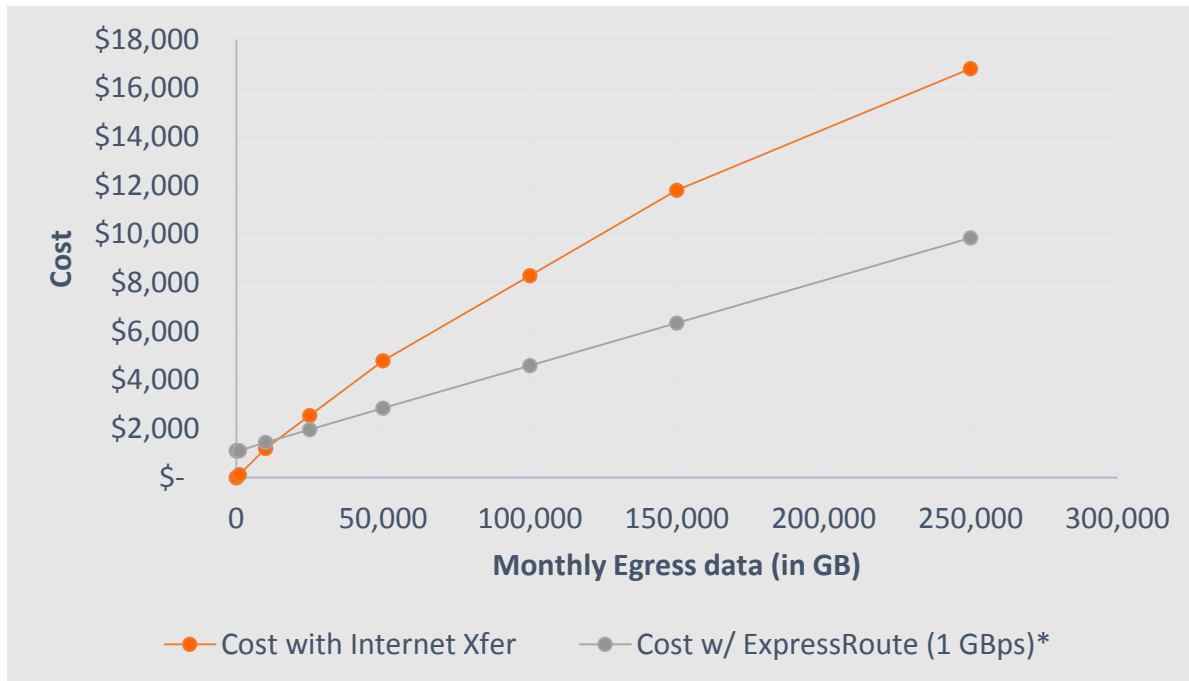
*Cost w/ ExpressRoute includes example monthly charge of $600 for the partner

Hybrid Applications

ExpressRoute is not just for deploying infrastructure and server workloads directly in the cloud. Building hybrid applications and workloads where resources or services reside on-premises and in the cloud is strategic for many organizations and is easily enabled using ExpressRoute. Additionally, Microsoft Azure application and data services such as Cloud Services, Storage and SQL Database are compatible and available to your application developers over your private ExpressRoute circuit. This allows you to build the next generation of hybrid applications using the latest capabilities by providing private and secure access to these services over your ExpressRoute circuit.

See the ExpressRoute FAQ for a complete list of Microsoft Azure public services supported with ExpressRoute.

Cross Region Connectivity

It is easy to deploy virtual machines, cloud services and Azure public services within separate Microsoft Azure regions (on the same continent) that can be connected to the same ExpressRoute circuit. This allows you to deploy infrastructure in multiple Microsoft Azure regions that can take advantage of your ExpressRoute circuit while only connecting your on-premises infrastructure to Azure and minimizing costs by eliminating bandwidth expenses between regions.

Consistent Network Performance

Microsoft Azure ExpressRoute offers circuits with bandwidth starting from 10 Mbps to 10 Gbps depending on your ExpressRoute provider. These connections are dedicated from your network,

through your provider, and then to Microsoft Azure to ensure consistent performance. ExpressRoute is highly available by supporting active-active router configurations and also provides control for how data is routed. This can provide you a more reliable and consistent experience over traditional Internet based connections.

Comparing ExpressRoute Provider Models

There are two types of providers you can choose from when using ExpressRoute: Connecting through an Exchange Provider (IXP) or a Network Service Provider (Telco).

Exchange Provider Overview

Exchange Providers allow you to connect your co-located hardware and your data center directly to Microsoft Azure. Exchange providers have bandwidth options starting from 200 Mbps through 10 Gbps. Connecting your datacenter to Microsoft Azure through an Exchange Provider requires a regional carrier or direct Ethernet connection to the exchange provider and from the exchange provider you will peer with Microsoft Azure. Choosing an exchange providers puts you in full control of the routing and availability with the management of the routers connecting to ExpressRoute in your hands.

To ensure your ExpressRoute circuit is highly available, Microsoft Azure provides two redundant ports on two routers in an active-active configuration to your on-premises network. When connecting through an exchange provider it is recommended to deploy redundant routers in your network in a highly available active-active configuration as well. With redundancy on both sides of the circuit you will avoid single points of failures and ensure your circuit is highly available.

Connecting through an Exchange Provider
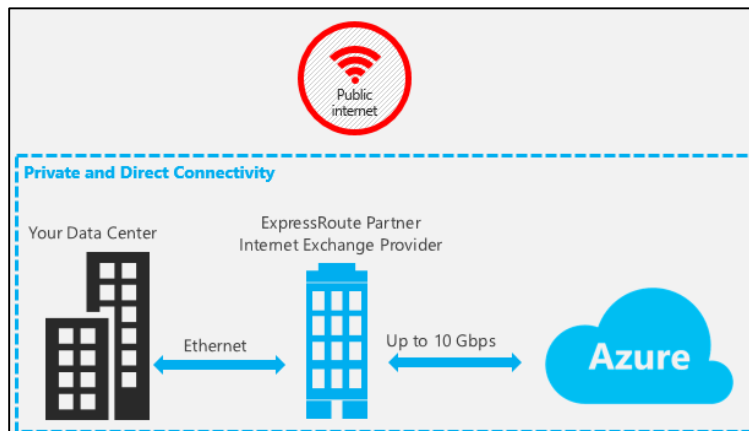
Network Service Provider Overview

Network Service Providers offer bandwidth options from 10 Mbps through 1 Gbps. With a Network Service Provider as your ExpressRoute partner setting up the routing and high availability is done for you and managed by your provider. Once connected, your infrastructure in Microsoft Azure and other Microsoft Azure services such as storage and SQL Database will be available to your network over your private ExpressRoute circuit.

Connecting through a Network Service Provider
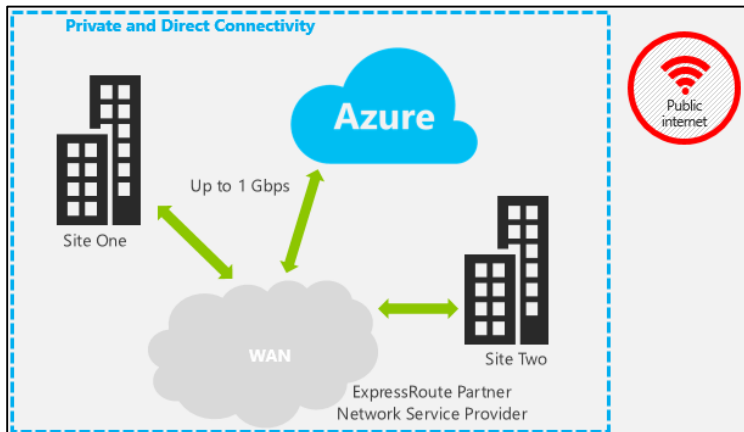
Comparing Service Provider Models

	Exchange Provider	Network Service Provider
Bandwidth	200 Mbps, 500 Mbps, 1 Gbps, 10 Gbps	10 Mbps, 50 Mbps, 100 Mbps, 500 Mbps, 1 Gbps
Routing	Managed by the customer	Managed by the provider
High Availability	Managed by the customer	Managed by the provider
Pricing	Pricing Details	Pricing Details
MPLS Support	No	Yes
Bandwidth Costs	Inbound and some outbound included	Inbound and outbound included

Choosing a Provider

You will need to establish a relationship with an ExpressRoute partner to establish connectivity to Microsoft Azure using ExpressRoute.

Click here to view the current list of ExpressRoute partners and supported bandwidth options.

Understanding Availability

Choosing either model, your ExpressRoute dedicated circuits are guaranteed to be available for use for a minimum of 99.9% of the time. If your circuit connectivity does not meet this guarantee and the cause is within Microsoft's control and not excluded in the ExpressRoute service level agreement you could be eligible for a service credit.

Click here to review the full details of the ExpressRoute service level agreement.

Identifying Provider Locations and Capabilities

Using the Microsoft Azure ExpressRoute PowerShell cmdlets you can view all of the available providers, locations and available bandwidths.

Installing and Configuring the Microsoft Azure PowerShell Cmdlets

After installing the Microsoft Azure PowerShell cmdlets, you will need to load the modules into your PowerShell session.

```
Import-Module 'C:\Program Files (x86)\Microsoft SDKs\Windows
Azure\PowerShell\Azure\Azure.psd1'

Import-Module 'C:\Program Files (x86)\Microsoft SDKs\Windows
Azure\PowerShell\Azure\Expressroute.psd1'
```

Using PowerShell to Enumerate ExpressRoute Providers and Capabilities

The **Get-AzureDedicatedCircuitServiceProvider** cmdlet returns a complete list of ExpressRoute providers.

```
Get-AzureDedicatedCircuitServiceProvider
```

```
DedicatedCircuitBandwidths DedicatedCircuitLocations  Name              Type
-------------------------- -------------------------  ----              ----
{Microsoft.WindowsAzure... Silicon Valley,Washingt... AT&T              Telco
{Microsoft.WindowsAzure... London                     British Telecom   Telco
{Microsoft.WindowsAzure... Silicon Valley,Washingt... Equinix           IXP
{Microsoft.WindowsAzure... Columbia1 DC               MSIT              Telco
{Microsoft.WindowsAzure... Silicon Valley,Washingt... Verizon           Telco
```

Running the following PowerShell code will allow you to filter on the selected provider and show the available bandwidths available. In this example, I am filtering the available bandwidths with the Equinix provider.

```
Get-AzureDedicatedCircuitServiceProvider |
      where Name -eq "Equinix" |
      select -ExpandProperty DedicatedCircuitBandwidths
```

```
Bandwidth Label
--------- -----
      200 200Mbps
      500 500Mbps
     1024 1024Mbps
```

The same cmdlet with a similar expression can be used to expend the available data center locations.

```
Get-AzureDedicatedCircuitServiceProvider |
      where Name -eq "Equinix" |
      select -ExpandProperty DedicatedCircuitLocations
```

```
Silicon Valley,Washington DC,London
```

Private Access to Microsoft Azure

Microsoft Azure ExpressRoute uses Border Gateway Protocol (BGP) for the exchange of routing information between your on-premises networks and Microsoft Azure. Networks use BGP to exchange

routing information through a process called peering where the networks are known as autonomous systems exchange routing information with each other.

With ExpressRoute you can configure access to your virtual machines and cloud services hosted in a virtual network and route traffic to them exclusively over your ExpressRoute circuit where the traffic never enters the public Internet. This exchange of routing information between your network on-premises and your network in Microsoft Azure is known as private peering.

In addition to connecting to virtual networks in Microsoft Azure over your ExpressRoute circuit you may also route traffic to Microsoft Azure services such as Microsoft Azure Storage and SQL Database. This allows you to access publicly accessible services without the worry of your data leaving your ExpressRoute circuit and network provider. This exchange of routing information between your network on-premises and Microsoft Azure public services is known as public peering.

Deploying ExpressRoute through a Network Service Provider (Telco)

It is assumed that at this point you already have an existing relationship and MPLS VPN setup over your wide area network with a network service provider such as AT&T, British Telecom, Level 3 or Verizon.

The first step to begin setting up connectivity is to use the Microsoft Azure PowerShell cmdlet **New-AzureDedicatedCircuit** to create the circuit.

```
New-AzureDedicatedCircuit -CircuitName "1GpsCircuit" `
                          -Bandwidth "1024" `
                          -Location "Silicon Valley" `
                          -ServiceProviderName "AT&T"
```

When the circuit has been created PowerShell will return the details of the circuit which includes the speed, name, location, service provider, status and service key.

The service key value is important because it uniquely identifies this specific circuit. This value will be needed when contacting your ExpressRoute provider so they can identify the circuit to provision. This service key will also be used when linking virtual networks and any management operations on the circuit such as deleting it. It is important to only share the service key with users that are authorized for changing your Microsoft Azure ExpressRoute configuration.

```
Bandwidth                        : 1024
CircuitName                      : 1GpsCircuit
Location                         : Silicon Valley
ServiceKey                       : e8b96590-3aae-40a2-9be5-4804a00139e2
ServiceProviderName              : at&t
ServiceProviderProvisioningState : NotProvisioned
Status                           : Enabled
```

Important: Billing starts the moment the circuit has been created!

Contacting your Network Service Provider

Once the circuit has been created you will need to contact your service provider by filling out an online form in their customer portal to request them to complete the connection on their end.

You will need to provide them the service key from the newly created circuit and to provide a /29 subnet that is outside of the IP addresses for your on-premises and Microsoft Azure Virtual Networks. This network will be split up by the provider into multiple /30 subnets and used to enabling routing.

Example Routing Subnet: 172.16.0.0/29

After your provider has completed the provisioning process you will see your circuit provisioning state is set to **Provisioned** in the output of the **Get-AzureDedicatedCircuit** cmdlet.

```
Bandwidth                         : 1024
CircuitName                       : 1GpsCircuit
Location                          : Silicon Valley
ServiceKey                        : e8b96590-3aae-40a2-9be5-4804a00139e2
ServiceProviderName               : at&t
ServiceProviderProvisioningState  : Provisioned
Status                            : Enabled
```

The next step is to create and link your Microsoft Azure Virtual Networks to the circuit. Linking and configuring virtual networks is discussed here.

Deploying ExpressRoute through an Exchange Provider (IXP)

It is assumed at this point that you already have a relationship with the ExpressRoute partner.

The next step is to provision a circuit using the **New-AzureDedicatedCircuit** cmdlet. This cmdlet will need to know the name of the circuit you are creating, the bandwidth requested, location, and of course the provider name.

```
New-AzureDedicatedCircuit -CircuitName "1GpsCircuit" `
                          -Bandwidth "1024" `
                          -Location "Silicon Valley" `
                          -ServiceProviderName "Equinix"
```

```
Bandwidth                         : 1024
CircuitName                       : 1GpsCircuit
Location                          : Silicon Valley
ServiceKey                        : 6b700120-5c30-47a3-a3f5-1a6ea715af7a
ServiceProviderName               : equinix
ServiceProviderProvisioningState  : NotProvisioned
Status                            : Enabled
```

Important: Billing starts the moment the circuit has been created!

Contacting Your Exchange Provider

After the circuit has been created using the PowerShell cmdlet you will need to copy the service key and pass it to your provider for them to complete the cross connect and enable the circuit.

To view the current status and service keys of your circuits you can run the **Get-AzureDedicatedCircuit** cmdlet without parameters to view all of your circuits or you can specify the circuit name to return only the details for the specified circuit.

Configuring Routing with an Exchange Provider

If your connection to ExpressRoute is through an Exchange Provider (IXP) it is your responsibility to setup and configure your router to exchange routes with Microsoft Azure.

After your provider has created the proper cross connects your circuit provisioning status will show **Provisioned** and you can then move on to configuring BGP routing.

`Get-AzureDedicatedCircuit`

```
Bandwidth                          : 1024
CircuitName                        : 1GpsCircuit
Location                           : Silicon Valley
ServiceKey                         : 6b700120-5c30-47a3-a3f5-1a6ea715af7a
ServiceProviderName                : equinix
ServiceProviderProvisioningState   : Provisioned
Status                             : Enabled
```

Routing IP Prefixes

ExpressRoute uses Border Gateway Protocol (BGP) for exchanging routes between your network and Microsoft Azure. To setup the required BGP sessions for public and private peering you will need to four /30 subnets for your primary and secondary routers for both the public and private peering configuration.

Note: The IP Prefixes for BGP cannot overlap with the IP prefixes within your virtual or on-premises networks.

Example Routing Subnets and VLAND IDs

Router	IP Prefix	Peering	VLAN ID
Primary	172.16.1.0/30	Private	555
Secondary	172.16.2.0/30	Private	555
Primary	172.16.1.4/30	Public	556
Secondary	172.16.2.4/30	Public	556

The first available IP address of each subnet will be assigned to your router and the second available IP address will be automatically assigned to the router on the Microsoft Azure side.

Router Configuration IP Address Assignments

	Customer Router	Microsoft Azure Router
Primary	172.16.1.1	172.16.1.2
Secondary	172.16.2.1	172.16.2.2
Primary	172.16.1.5	172.16.1.6
Secondary	172.16.2.5	172.16.2.6

Example Deployment
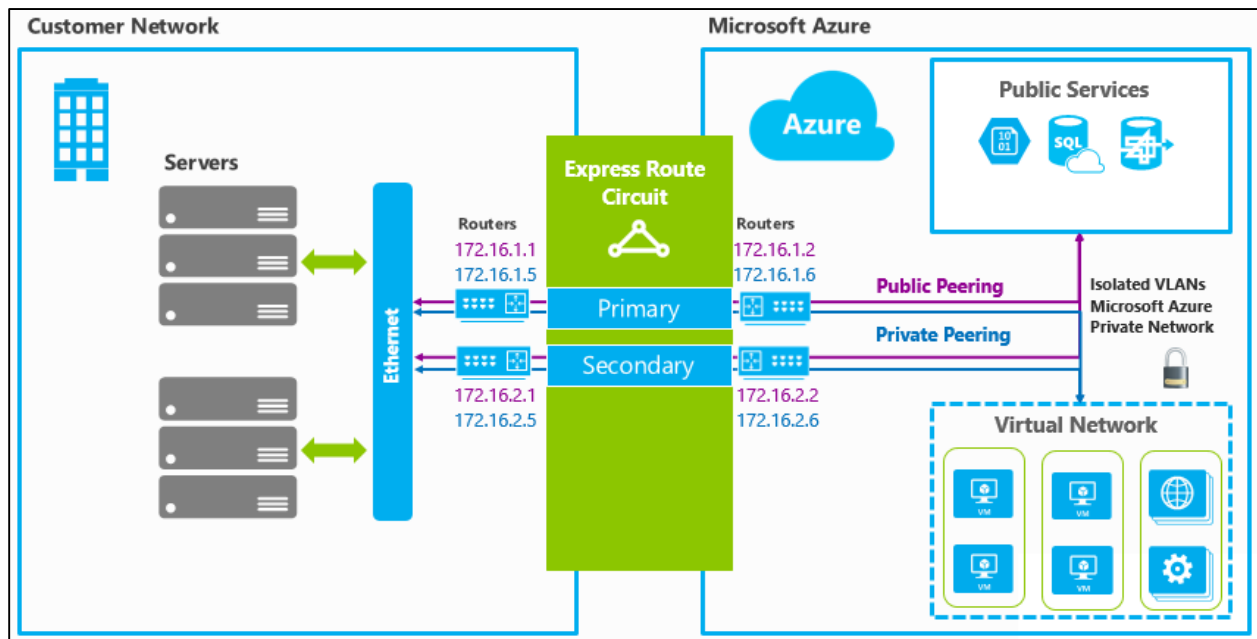
Autonomous System Number

To configure BGP for ExpressRoute you will need to provide an autonomous system number (ASN) to represent your network. You can use a public ASN that you own or you can use a private ASN as long as it is greater than 65000.

Configuring Border Gateway Protocol (BGP) Peering

To configure the BGP sessions for both private and public peering you can use the Microsoft Azure PowerShell cmdlets.

The following sample uses example information on how you could configure BGP sessions for both private and public peering in the Exchange Provider model.

To execute the script you will need to replace the place holder value for your service key by retrieving that value using the **Get-AzureDedicatedCircuit** cmdlet. The **New-AzureBGPPeering** cmdlet supports passing a **-SharedKey** parameter with an MD5 hash password to ensure only authenticated devices can manipulate routes. The hash must be a 16-byte hash value represented as a 32 digit hexadecimal number.

Using PowerShell to Configure BGP Peering for an Exchange Provider

```
# Service key from your previously created and provisioned circuit
$ServiceKey = "[your service key goes here]"

# MD5 Hash to authenticate BGP sessions
$MD5Hash = "[your MD5 hash password]"

# Subnets used for configuring private peering
$private_Subnet_Primary   = "172.16.1.0/30"
$private_Subnet_Secondary = "172.16.2.0/30"

# Subnets used for configuring public peering
$public_Subnet_Primary    = "172.16.1.4/30"
```

```
$public_Subnet_Secondary  = "172.16.2.4/30"

# Autonomous System Number
$ASN = "65520"

# VLAN ID for private peering
$VLANPrivate = "555"

# VLAN ID for public peering
$VLANPublic = "556"

# Create the private peering configuration
New-AzureBGPPeering -ServiceKey $ServiceKey `
                    -PrimaryPeerSubnet $private_Subnet_Primary `
                    -SecondaryPeerSubnet $private_Subnet_Secondary `
                    -PeerAsn $ASN `
                    -VlanId $VLANPrivate `
                    -AccessType Private `
                    -SharedKey $MD5Hash


# Create the public peering configuration
New-AzureBGPPeering -ServiceKey $ServiceKey `
                    -PrimaryPeerSubnet $public_Subnet_Primary `
                    -SecondaryPeerSubnet $public_Subnet_Secondary `
                    -PeerAsn $ASN `
                    -VlanId $VLANPublic `
                    -AccessType Public `
                    -SharedKey $MD5Hash
```

Some guidelines for configuring BGP when connecting to Microsoft Azure ExpressRoute

- You may publish up to 3000 routes to the Microsoft Azure routers for private peering and up to 4000 for public peering. You should aggregate routes to stay within this limit.
- The smallest subnet you should publish is a /29.
- Do not publish private IP addresses through the public peering.

Virtual Network Configuration

After your ExpressRoute circuit has been provisioned you will need to create and link one or more virtual networks to the circuit. You can link multiple virtual networks to an ExpressRoute circuit from any region on the same continent. For example: West US and East US may connect directory as well as North Europe and West Europe. However, virtual networks created in West US and North Europe could not be linked together on the same circuit.

Specifying Address Spaces

To configure ExpressRoute you must specify the address spaces or IP prefixes for your on-premises and Microsoft Azure-based Virtual Networks. The address spaces should not overlap.

Local Network Prefixes

The IP Prefixes used on your on-premises network configuration can include public or private IP prefixes. When configuring your virtual network you should add all of the IP prefixes you wish to be able to communicate to the Microsoft Azure Virtual Network.

IP Prefixes for On-Premises or Co-Located Network

NAME	ADDRESS SPACE			
ONPREM	ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
VPN DEVICE IP ADDRESS	216.221.239.232/28	216.221.239.232	/28 (16)	216.221.239.224 - 216.221.239.239
0.0.0.0	add address space			

Note: When creating a virtual network using the management portal you are currently required to specify an IP address for the VPN device. This value is not used with ExpressRoute and any placeholder address can be used such as 0.0.0.0.

Virtual Network Prefixes

The IP prefixes that will be used within your Microsoft Azure Virtual Network(s) should not overlap with your on-premises network connected to Microsoft Azure. Only IP prefixes from RFC1918 are supported within Microsoft Azure Virtual Networks.

Available Ranges for Microsoft Azure Virtual Networks

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)

As part of creating your virtual network you should partition your address space into subnets.

Note: You must create a /28 subnet named Gateway for the Microsoft Azure gateway roles.

Example IP Prefixes for a Microsoft Azure Virtual Network

Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/16	10.0.0.0	/16 (65536)	10.0.0.0 - 10.0.255.255
SUBNETS			
APP	10.0.0.0	/24 (256)	10.0.0.0 - 10.0.0.255
DATA	10.0.1.0	/24 (256)	10.0.1.0 - 10.0.1.255
Gateway	10.0.2.8	/28 (16)	10.0.2.0 - 10.0.2.15
DNS	10.0.2.16	/29 (8)	10.0.2.16 - 10.0.2.23
add subnet	add gateway subnet		

Linking a Virtual Network to an ExpressRoute Circuit

After the ExpressRoute circuit is provisioned and configured, the next step is to link a virtual network to your ExpressRoute circuit.

Call the **New-AzureDedicatedCircuitLink** cmdlet and specify the service key and the virtual network name you want to link to the circuit. After this command has completed routes from your virtual network will be advertised to your routers to allow connectivity over the ExpressRoute circuit.

Linking a Virtual Network to the ExpressRoute Circuit

```
New-AzureDedicatedCircuitLink -ServiceKey $ServiceKey -VNetName "ExpressRouteVNET"

                                          State VnetName
                                          ----- --------
                                      Provisioned ExpressRouteVNET
```

Connecting Multiple Virtual Networks to the Same Circuit

You can connect virtual networks to the same ExpressRoute circuit within the same physical geography.

Currently Available Virtual Network to Virtual Network Locations:

- West US, East US and Central US
- West Europe and North Europe

Accessing Public and Private Services from an ExpressRoute circuit in multiple regions
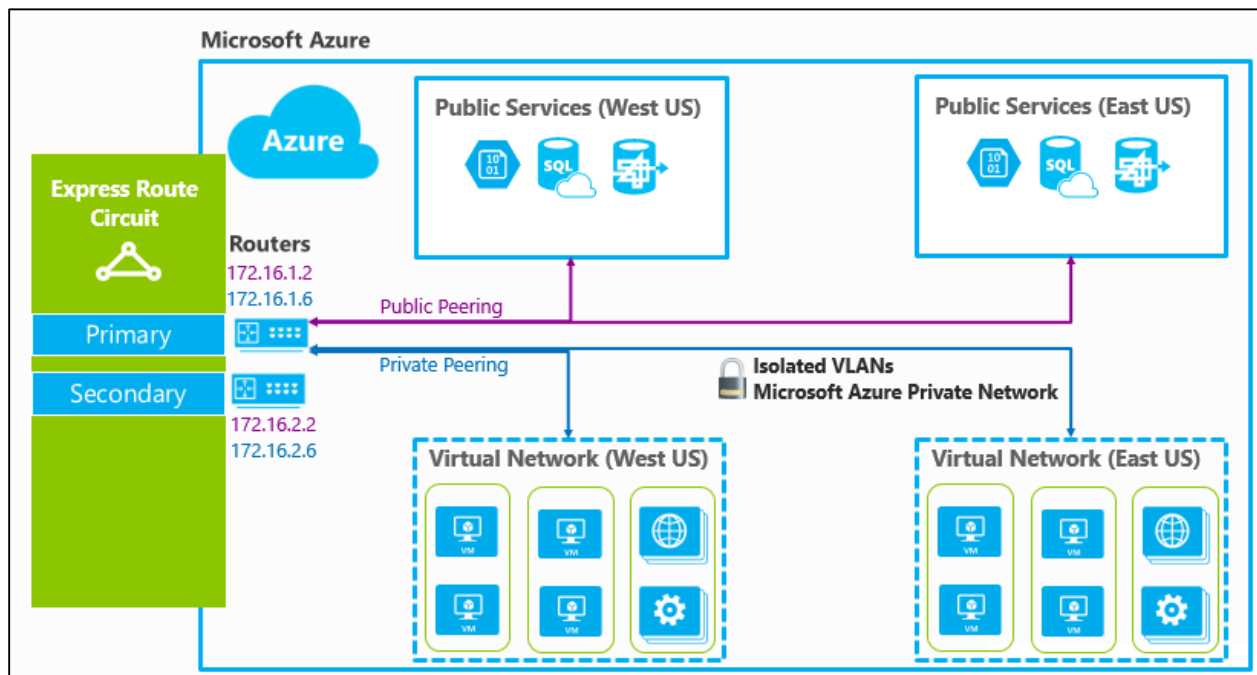
Example Virtual Network to Virtual Network Configuration

Local Network	ExpressRouteVNET (West US)	ExpressRouteVNETEast (East US)
216.221.239.232/28	10.0.0.0/16	192.168.1.0/24

Linking a second virtual network in a remote region to the same ExpressRoute circuit.

```
New-AzureDedicatedCircuitLink -ServiceKey $serviceKey -VNetName "ExpressRouteVNETEast"
```

```
New-AzureDedicatedCircuitLink -ServiceKey $serviceKey -VNetName "ExpressRouteVNETEast"

                                            State VnetName
                                            ----- --------
                                        Provisioned ExpressRouteVNETEast
```

Compatibility

Currently, Microsoft Azure ExpressRoute is not compatible with site-to-site, point-to-site or regionally connected virtual networks. ExpressRoute is fully compatible with internal load balancing, static IPs, reserved IPs and public IPs.

Upgrading an Existing Circuit

The process of upgrading to a higher capacity circuit is relatively simple. Create and configure a new circuit with a higher capacity using the process outlined earlier. Once the circuit is ready, simply unlink the existing circuit from the virtual network and link it to the new circuit.

```
# Unlink the existing circuit from the virtual network
Remove-AzureDedicatedCircuitLink -ServiceKey $serviceKey -VNetName $vnetName

# Link the virtual network to the new circuit
New-AzureDedicatedCircuitLink -ServiceKey $upgradedServiceKey -VNetName $vnetName
```

Warning: Unlinking and relinking a circuit to a virtual network will cause a short amount of lost connectivity between your on-premises network and your virtual network.

Migrating Virtual Networks with Site to Site Gateways to ExpressRoute

It is possible to move an existing Microsoft Azure Virtual Network that currently uses a site-to-site VPN gateway to use an ExpressRoute circuit. The steps to migrate an existing configuration are below.

Delete the Existing Gateway

Delete the existing gateway by pressing the **DELETE GATEWAY** button in the portal or by using the **Remove-AzureVNETGateway** PowerShell cmdlet.

Deleting an Existing Site-to-Site Gateway from the management portal.
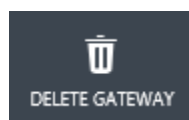
Resize the Existing Gateway Subnet

Existing site to site gateways support a gateway subnet with a minimum size of a /29. However, Microsoft Azure ExpressRoute gateways support a minimum gateway subnet size of /28. Change the subnet to support the increased size and save your virtual network configuration.

**Site-to-Site gateway subnet before resizing (/29)**

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.2.0/24	192.168.2.0	/24 (251)	192.168.2.4 - 192.168.2.254
SUBNETS			
App	192.168.2.0	/25 (123)	192.168.2.4 - 192.168.2.126
Gateway	192.168.2.128	/29 (3)	192.168.2.132 - 192.168.2.134

add subnet   add gateway subnet

Site-to-Site Gateway subnet after resizing (/28)

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
192.168.2.0/24	192.168.2.0	/24 (251)	192.168.2.4 - 192.168.2.254
SUBNETS			
App	192.168.2.0	/25 (123)	192.168.2.4 - 192.168.2.126
Gateway	192.168.2.128	/28 (11)	192.168.2.132 - 192.168.2.142

add subnet   add gateway subnet

Enable ExpressRoute on the Gateway

After the existing site-to-site gateway has been deleted and the gateway subnet has been resized you can then enable ExpressRoute by checking the **Use ExpressRoute** check box in the management portal and then clicking save.
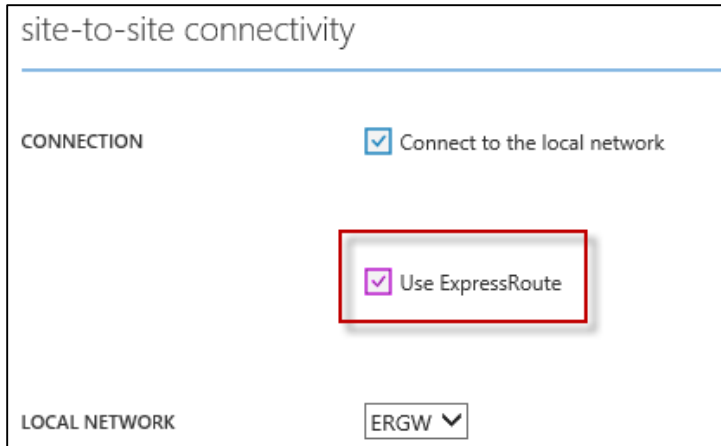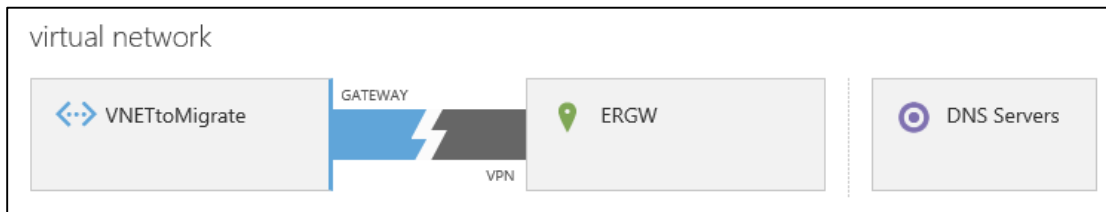
Create the Gateway and Link the Virtual Network to ExpressRoute

To complete the migration from site-to-site to ExpressRoute you must click the **CREATE GATEWAY** button to recreate the gateway.

Once the gateway has completed provisioning simply link the virtual network to your existing ExpressRoute circuit.

Gateway recreated with ExpressRoute Enabled.

Note: with ExpressRoute the portal does not currently show a connected state when ExpressRoute is connected.

New-AzureDedicatedCircuitLink –ServiceKey $serviceKey –VNetName "VNETtoMigrate"


Warning: Migrating an existing virtual network from site-to-site to ExpressRoute will cause a short amount of lost connectivity between your on-premises network and your virtual network.

Securing ExpressRoute

Microsoft Azure ExpressRoute is more secure than a traditional Internet connection due to the private and dedicated nature of its connection. However, there are several additional approaches that you can utilize to decrease your attack surface and lower the risk of your network being attacked.

## Firewalls and Security Appliances

Microsoft Azure ExpressRoute places you in control of your network. This means you can place additional firewalls, security appliances or further protect your network with IPSEC.
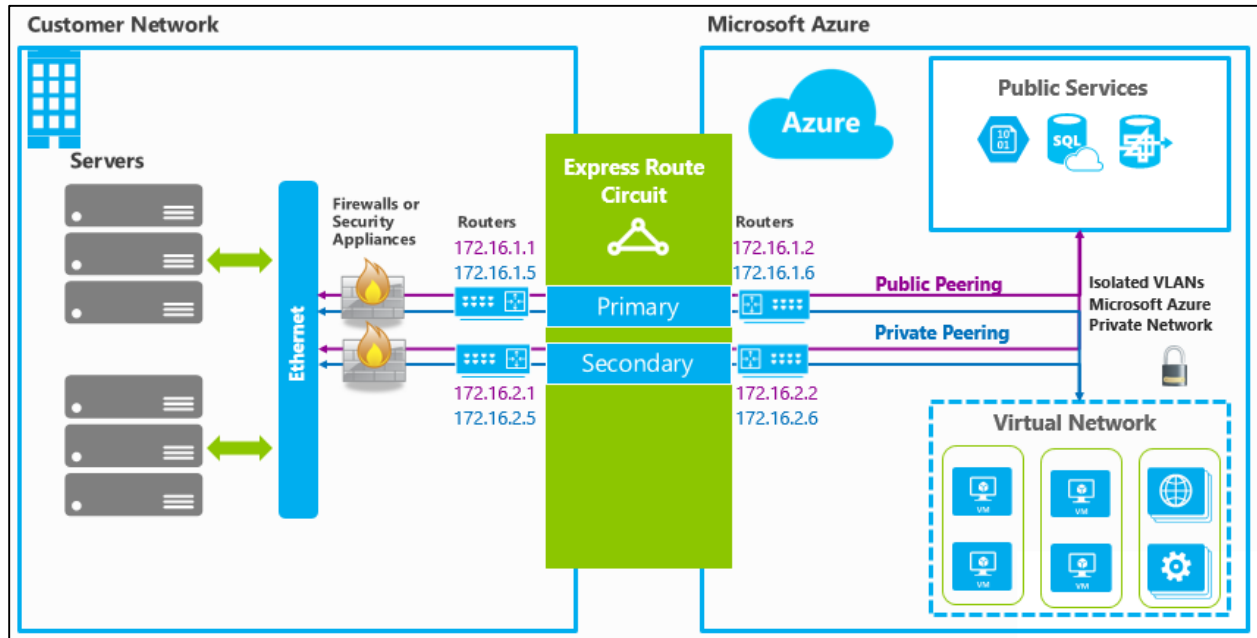
Securing External Endpoints

When creating virtual machines in Microsoft Azure, endpoints are automatically created for Remote Desktop and Remote PowerShell for Windows-based virtual machines and SSH for Linux-based virtual machines. You can further secure access to these virtual machines by removing the endpoints altogether and accessing the management features using the virtual machines internal IP address from your ExpressRoute network.

Managing Virtual Machines by connecting direct over an ExpressRoute Circuit.
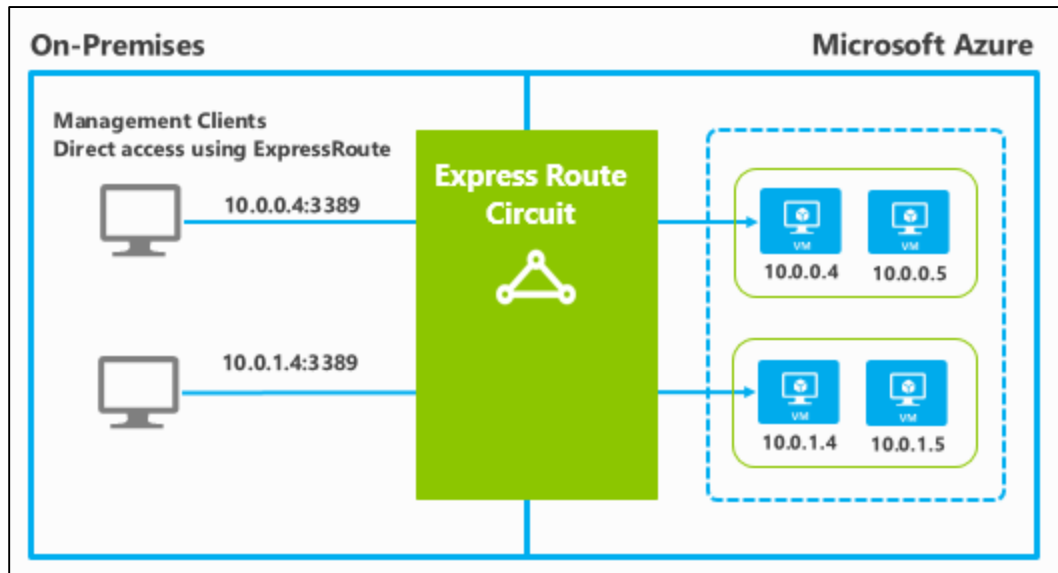
Using Access Control Lists

If management endpoints on Microsoft Azure Virtual Machines are required to be exposed to external networks it is highly recommended to do so only using access control lists to restrict the visibility and access to the these ports to a whitelist of IP addresses or networks.

Managing Virtual Machines by connecting to internal IP addresses for internal management and external endpoints with an access control list (ACL) for external access.
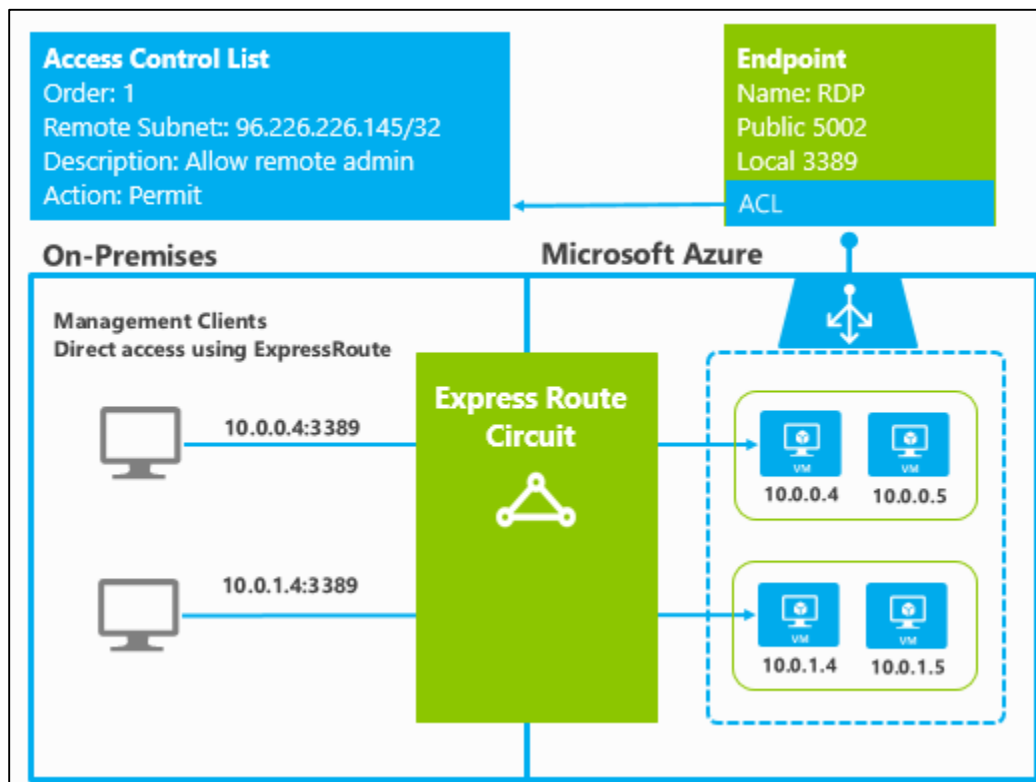
Removing an ExpressRoute Circuit

Billing for your ExpressRoute circuit begins once the circuit has been created regardless of its provisioned state. To remove an ExpressRoute circuit and stop billing it is important to include your service provider as part of the disconnect process.

To remove a provisioned circuit follow the following steps:

Remove the link from any virtual networks using the **Remove-AzureDedicatedCircuitLink** cmdlet.

Contact your service provider with the service key for the specific circuit you wish to remove. You can use the **Get-AzureDedicatedCircuit** cmdlet to retrieve the service key.

Once your service provider notifies you that the cross connects have been removed the circuits provisioning state should be set to NotProvisioned. You can view the state by calling the **Get-AzureDedicatedCircuit** cmdlet.

Finally, call the **Remove-AzureDedicatedCircuit** cmdlet passing the service key to delete the circuit from your subscription.

Summary

Microsoft Azure ExpressRoute provides private and consistent network capabilities to enable the hybrid cloud with Microsoft Azure.

ExpressRoute is ideal for workloads that require transferring large amounts of data, low latency, or solutions that require a higher degree of security, privacy and control over the network. ExpressRoute may also provide significant cost savings related to bandwidth costs by providing a lower cost alternative for high bandwidth workloads.

ExpressRoute also enables you to connect virtual machines and public services from multiple Microsoft Azure regions directly to your on-premises network providing hybrid cloud capabilities and enabling you to bring your infrastructure closer to your customers.