**Solution Design Document**

Intact US Insurance Limited

Azure Network Design

Oct 05, 2021

Version 0.1

Table of Contents

[**About This Design Process** 4](#_Toc84611068)

[**Document History** 4](#_Toc84611069)

[Document Review 5](#_Toc84611070)

[Introduction 5](#_Toc84611071)

[How does ExpressRoute help? 6](#_Toc84611072)

[Network Privacy 6](#_Toc84611073)

[Reduces Costs 6](#_Toc84611074)

[Cross Region Connectivity 6](#_Toc84611075)

[Consistent Network Performance 6](#_Toc84611076)

[ExpressRoute Provider Model 7](#_Toc84611077)

[Network Service Provider Overview 7](#_Toc84611078)

[Private Access to Microsoft Azure 7](#_Toc84611079)

[Deploying ExpressRoute through a Network Service Provider (Telco) 8](#_Toc84611080)

[Routing IP Prefixes 8](#_Toc84611081)

[Requirement 9](#_Toc84611082)

[Option1: Private peering to single Azure region 10](#_Toc84611083)

[Option2: Private peering to single Azure region 11](#_Toc84611084)

[Optimized Routing: 12](#_Toc84611085)

[Virtual Network Configuration 12](#_Toc84611086)

[Specifying Address Spaces 12](#_Toc84611087)

[Local Network Prefixes 12](#_Toc84611088)

[IP Prefixes for On-Premises or Co-Located Network 13](#_Toc84611089)

[Virtual Network Prefixes 13](#_Toc84611090)

[Available Ranges for Microsoft Azure Virtual Networks 13](#_Toc84611091)

[Example IP Prefixes for a Microsoft Azure Virtual Network 14](#_Toc84611092)

[Securing Express Route 14](#_Toc84611093)

[Firewalls and Security Appliances 14](#_Toc84611094)

[Securing External Endpoints 14](#_Toc84611095)

[Using Access Control Lists 15](#_Toc84611096)

[Summary 15](#_Toc84611097)

### **About This Design Process**

|  |  |
| --- | --- |
| Author |  |
| Change Authority | <CCoE US> |
| Internal Reference | <Doc ID> |
| Project Name | Intact US Insurance Limited. |

### **Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | Reason for Change |
| 0.1 | 26/07/2019 | Draft | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Table 1 Document history*

### Document Review

After creating an initial draft, the design document will be peer reviewed internally. Internal peer reviewed document will have version less than 1 and customer released version will be greater than 1.

* As a standard offering the document will be once internally peer reviewed and once external/ customer peer reviewed.
* After peer review all comments/feedback will be captured in appendix A and then updated to the document as a final design.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Review Date | Description | Role | Reviewer |
|  |  |  |  |  |
|  |  |  |  |  |

# Introduction

Microsoft Azure ExpressRoute makes it easy to establish dedicated and private circuits between Intact US data center and Microsoft Azure. The infrastructure can be located on-premises in 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, the network circuit is isolated using industry standard VLANs to allow private, secure access to resources deployed in Microsoft Azure Virtual Networks and to provide connectivity to Microsoft Azure public services.

For more detailed information, please refer the Microsoft documentation

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

## How does ExpressRoute help?

### Network Privacy

Connectivity between 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 we 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.

### 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 provides control for how data is routed. This can provide you a more reliable and consistent experience over traditional Internet based connections.

## ExpressRoute Provider Model

### Network Service Provider Overview

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

|  |  |
| --- | --- |
| **Metrics** | **Network Service Provider** |
| Bandwidth | 10 Mbps, 50 Mbps, 100 Mbps, 500 Mbps, 1 Gbps |
| Routing | Managed by the provider |
| High Availability | Managed by the provider |
| MPLS Support | Yes |
| Bandwidth Costs | Inbound and outbound included |

### 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 onpremises 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 setup over your wide area network with a network service provider such as Level 3 or Verizon.

### 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 our virtual or on-premises networks.

Example Routing Subnets and VLAND IDs

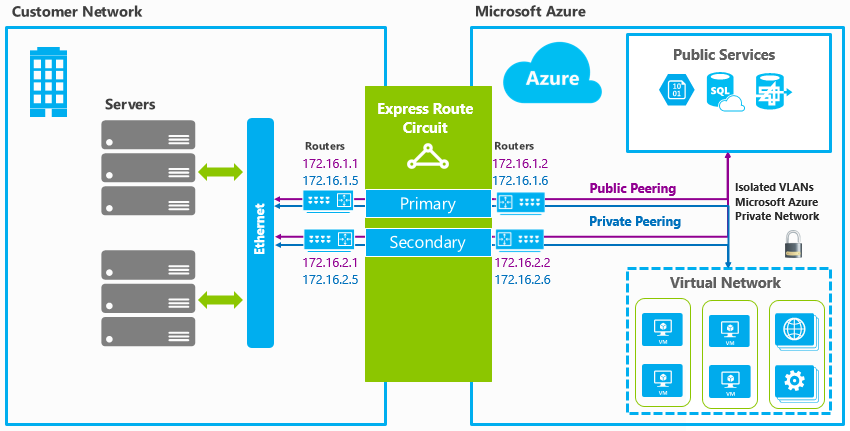
|  |  |  |  |
| --- | --- | --- | --- |
| **Router** | **IP Prefix** | **Peering** | **VLAN ID** |
| **Primary** | 172.16.1.0/30 | Private | 555 |
| **Secondary** | 172.16.2.0/30 | Private | 555 |
| **Primary** | 172.16.1.4/30 | Public | 556 |
| **Secondary** | 172.16.2.4/30 | Public | 556 |

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



# Requirement

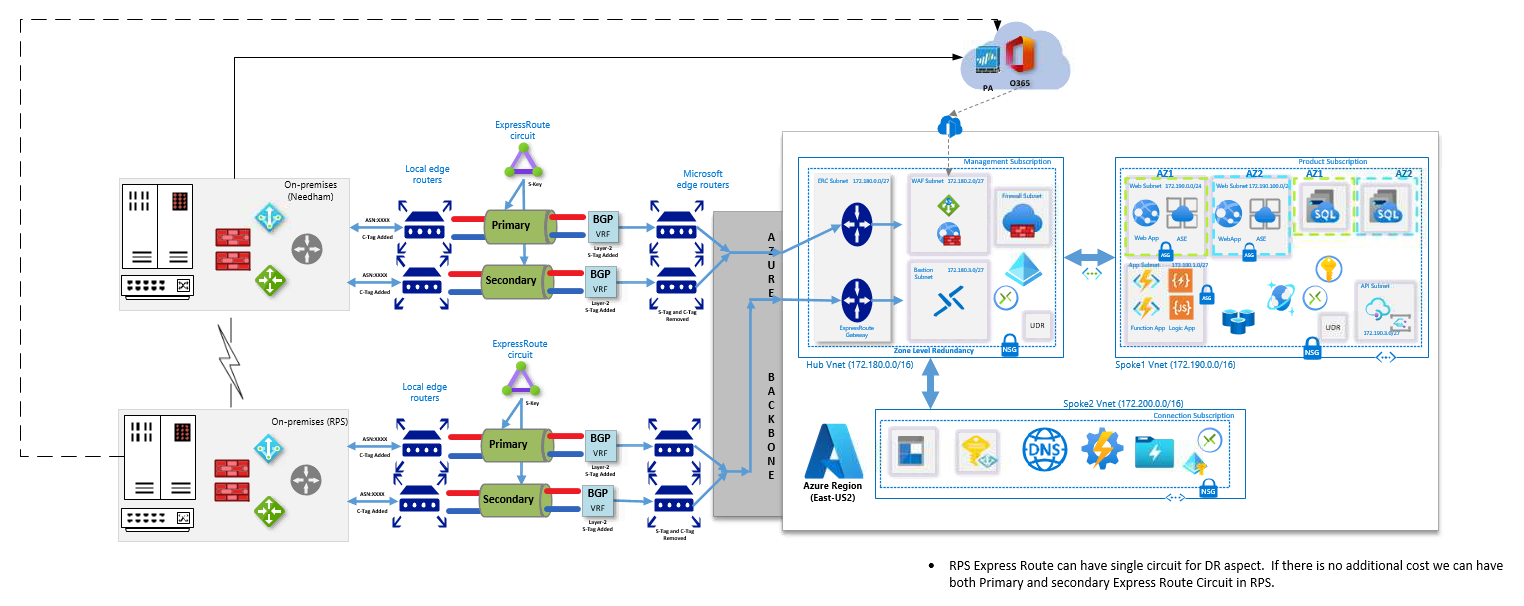
The customer needed complete isolation between the Azure prod/non-prod vNets. The Azure Hub and Spoke vNets had to be accessed as a direct connection from the Azure prod/non-prod vNets, but also could be accessed from on-prem directly if needed. The main requirements are,

1. Single region end-to-end redundancy with East US2
2. Azure Vnets to be consolidated within each subscription using appropriate options (Hub & Spoke Vnets)
3. Each Azure environment to connect to On-prem with dedicated private peering using Express Route Circuit
4. Each Shared Services environment to be utilised by each environment (Prod/Non-prod) via direct peering within the cloud, not traversing ExpressRoute.
5. Prod and Non-Prod environments can only interface via on-prem. Need to ensure prod and non-prod cannot talk to each other direct or by using the Shared Services vNet as transit.

We came up with a couple of options,

### Option1: Private peering to single Azure region

The diagram below uses Azure dedicated express route circuit (private site-to-site peering with the secure/direct connectivity) to the azure services using segmented Hub & Spoke reference architecture for underlying vNets from each logical infrastructure components. Furthermore, we can even extend it to the environments (Prod/Non-prod).



**Highlights:**

1. High availability within single Azure regions (Multi AZ’s Redundancy)
2. Complete isolation between Azure Management and Multiple Spoke Vnet

**Lowlights:**

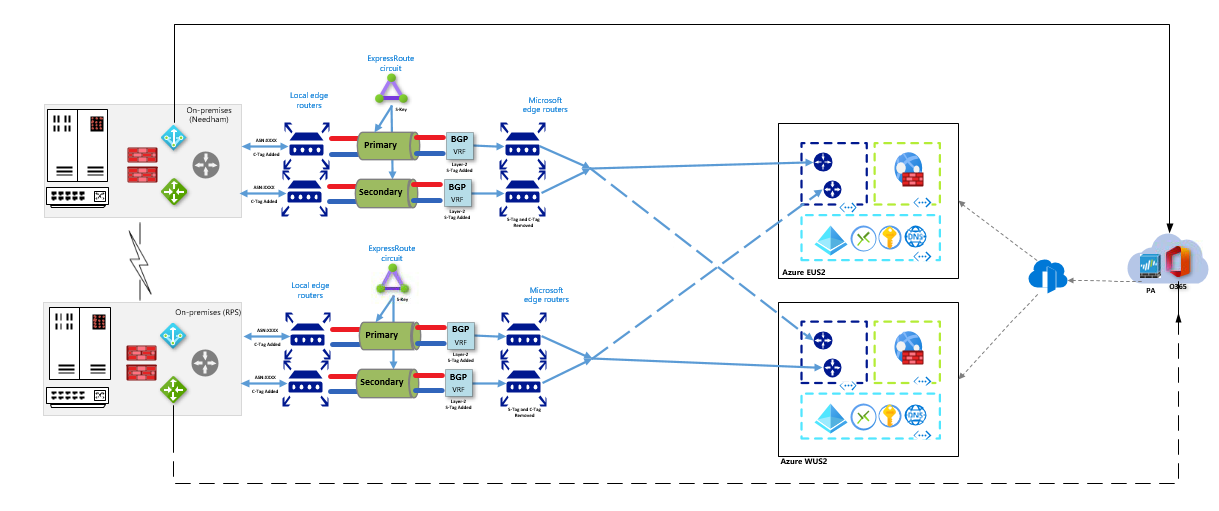
1. Expected low latency rate of 2-3 mins during on-premises region failovers (assuming 1GBPS direct connectivity)

**Next Focus:**

1. Aiming to enable BFD (Bi-directional Forward Link Detection) Failures towards increased network level monitoring for quicker resolution

### Option2: Private peering to single Azure region

The diagram below uses Azure dedicated express route circuit (private site-to-site peering with the secure/direct connectivity) to the azure services using cross connectivity between two azure regions with traditional segmented Hub & Spoke reference assuming DR in place which would minimize latency rates



**Highlights:**

1. Disaster recovery between two Azure regions (No Geo Replication)
2. High availability in each Azure region (Multi AZ’s Redundancy)
3. Complete isolation between Azure Management and Multiple Spoke Vnet

**Lowlights:**

1. Expected low latency rate of 2-3 mins during on-premises region failovers (assuming 1GBPS direct connectivity)

**Next Focus:**

1. Aiming to enable BFD (Bi-directional Forward Link Detection) Failures towards increased network level monitoring for quicker resolution

### Optimized Routing:

We can assign a higher weight to the local connection than to the remote connection

We can also influence routing from VNet to your on-premises network, if we have multiple ExpressRoute circuits, by configuring the weight of a connection instead of applying AS PATH prepending. For each prefix, we will always look at the connection weight before the AS Path length when deciding how to send traffic.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-optimize-routing>

# 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.

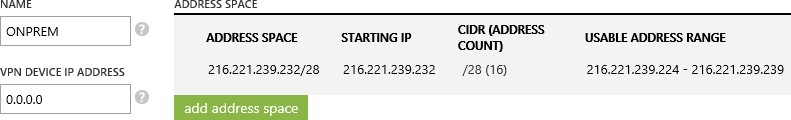
## Specifying Address Spaces

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



**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.

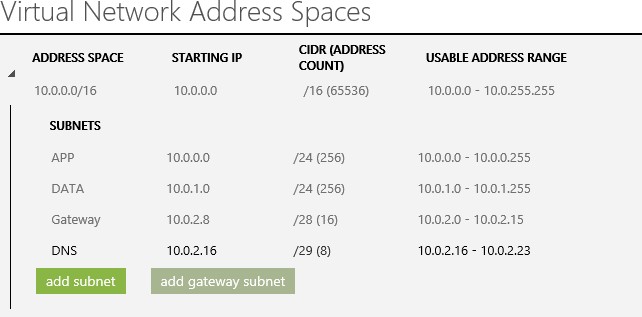
### Available Ranges for Microsoft Azure Virtual Networks

|  |  |
| --- | --- |
| 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 virtual network you should partition our 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



# Securing Express Route

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.

### 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.

# 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.