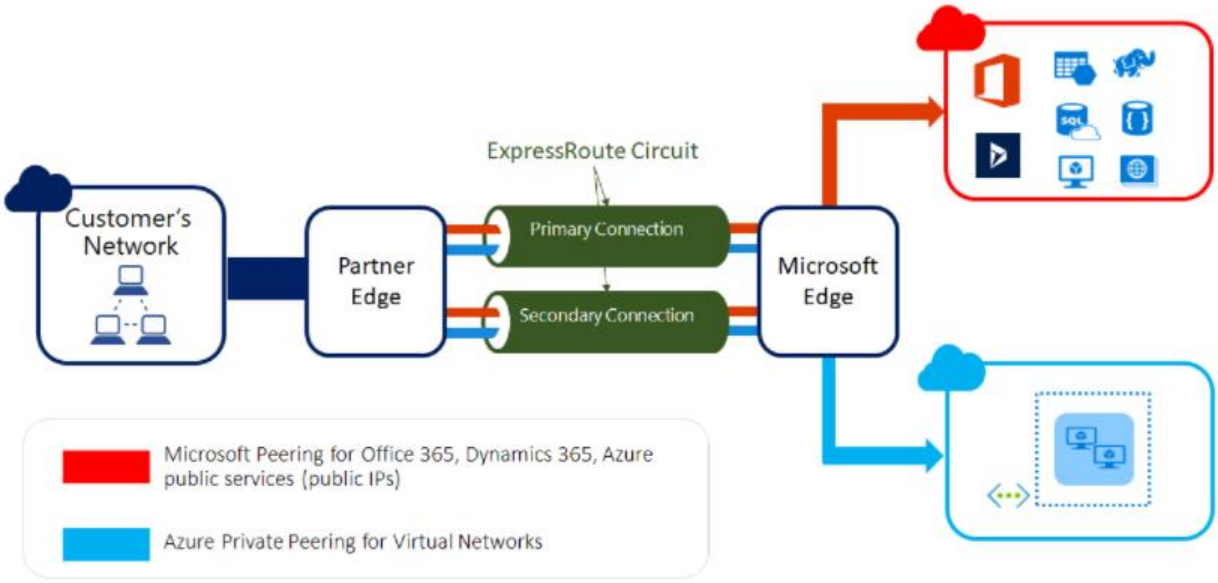
AZURE: EXPRESSROUTE CONECTIVITY MODELS

ExpressRoute extends on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365. Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility.

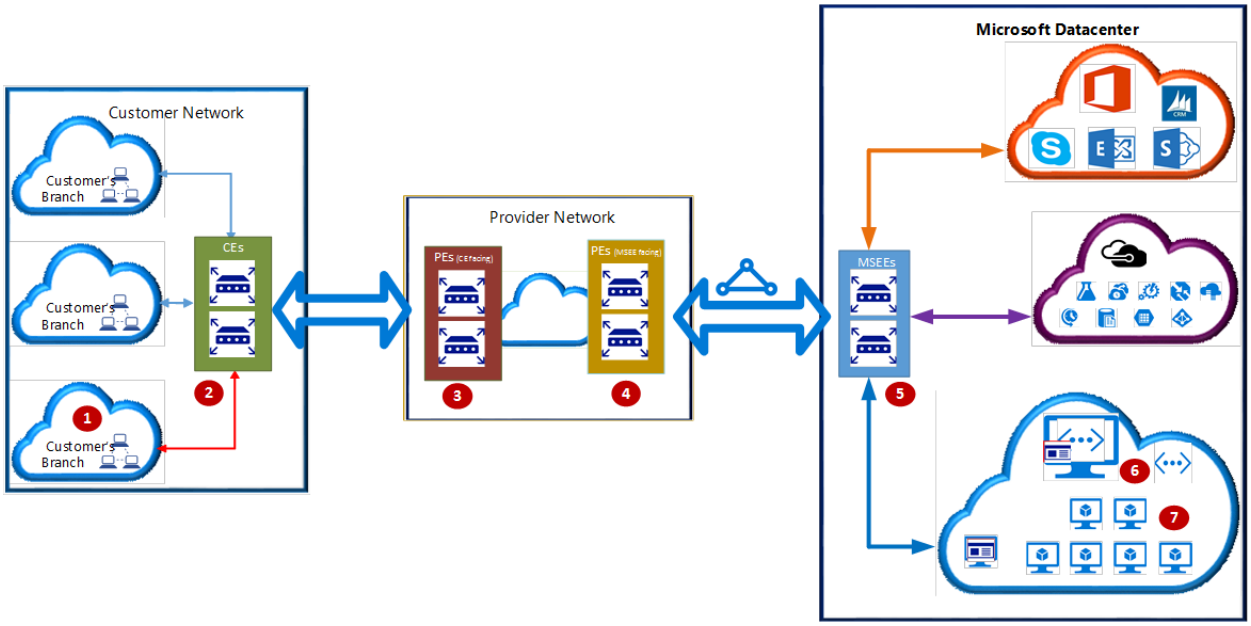


ExpressRoute connectivity traditionally involves three distinct network zones, as follows:

1. Customer Network
2. Provider Network
3. Microsoft Datacenter

In the ExpressRoute direct connectivity model (offered at 10/100 Gbps bandwidth), customers can directly connect to Microsoft Enterprise Edge (MSEE) routers' port. Therefore, in the direct connectivity model, there are only customer and Microsoft network zones.

The following diagram shows the logical connectivity of a customer network to Microsoft network using ExpressRoute.



In the ExpressRoute Service Provider connectivity model--Cloud Exchange Co-location, Point-to-Point Ethernet Connection, or Any-to-any (IPVPN)--the network points 3 and 4 may be switches (Layer 2 devices) or routers (Layer 3 devices).

In the direct connectivity model, there are no network points 3 and 4; instead CEs (2) are directly connected to MSEEs via dark fiber.

The key network points illustrated are as follows:

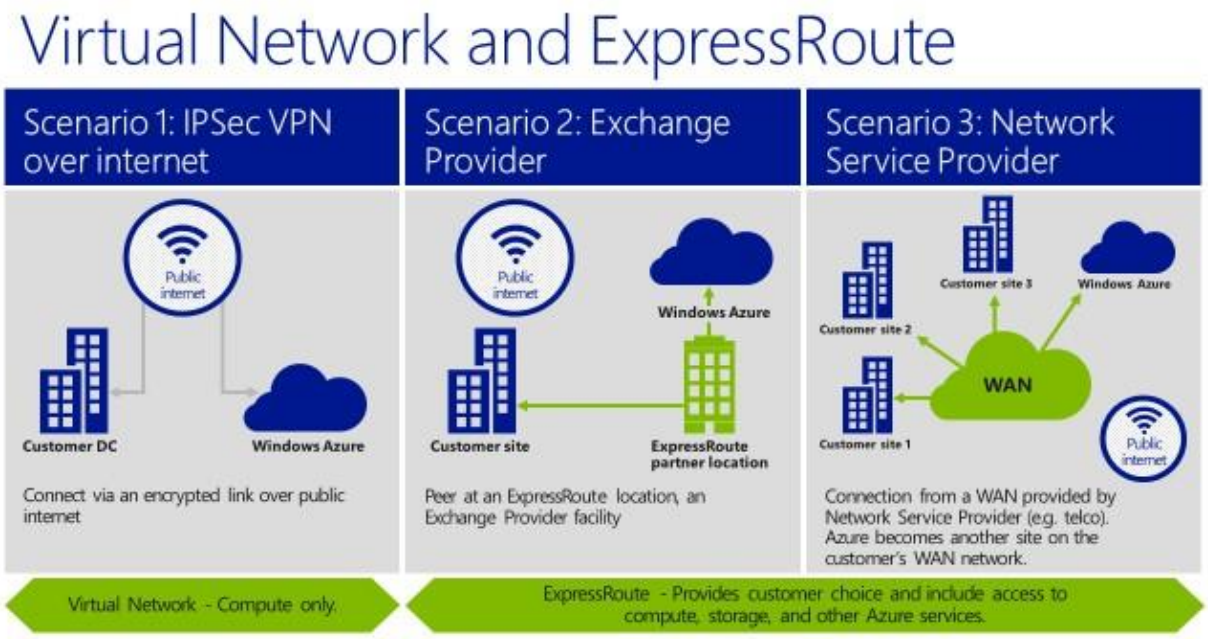
1. Customer compute device (for example, a server or PC)
2. CEs: Customer edge routers
3. PEs (CE facing): Provider edge routers/switches that are facing customer edge routers. Referred to as PE-CEs in this document.
4. PEs (MSEE facing): Provider edge routers/switches that are facing MSEEs. Referred to as PE-MSEEs in this document.
5. MSEEs: Microsoft Enterprise Edge (MSEE) ExpressRoute routers
6. Virtual Network (VNet) Gateway
7. Compute device on the Azure VNet

If the Cloud Exchange Co-location, Point-to-Point Ethernet, or direct connectivity models are used, CEs (2) establish BGP peering with MSEEs (5).

If the Any-to-any (IPVPN) connectivity model is used, PE-MSEEs (4) establish BGP peering with MSEEs (5). PE-MSEEs propagate the routes received from Microsoft back to the customer network via the IPVPN service provider network.

Previously

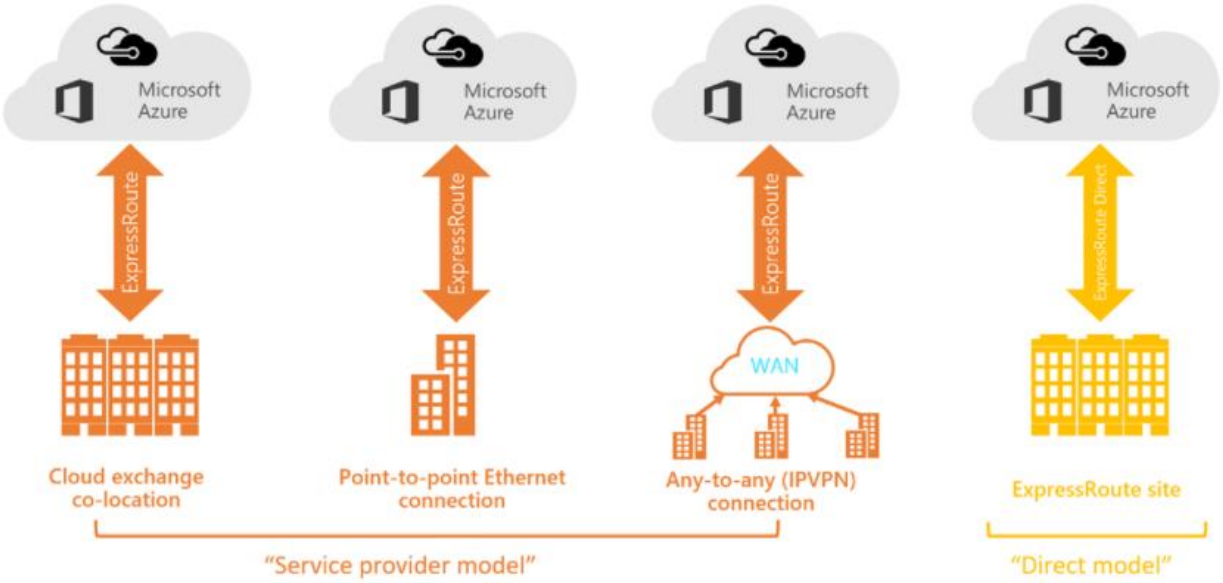
In the past we have three scenarios to connect to Azure:



Where the VPN connection over internet is the one everyone gets from the first minute of the discussion. Though the difference between the “Exchange Provider” and the “Network Service Provider” was often the real debate. Here the “Exchange Provider” was to be compared with a leased / direct connection, where you manage everything on top of that yourself. In OSI terms, you start from layer 2. The “Network Service Provider” concept was a managed concept, where you got a layer 3 solution (in OSI terms). The telecom provider took care of all the complexity for you. Ofcourse, there is a cost difference between both.

New Naming

If we take a look towards the Azure documentation, we notice a new visualization:



ExpressRoute Service Provider Model

You can create a connection between your on-premises network and the Microsoft cloud in three different ways via “Service Provider Model”.

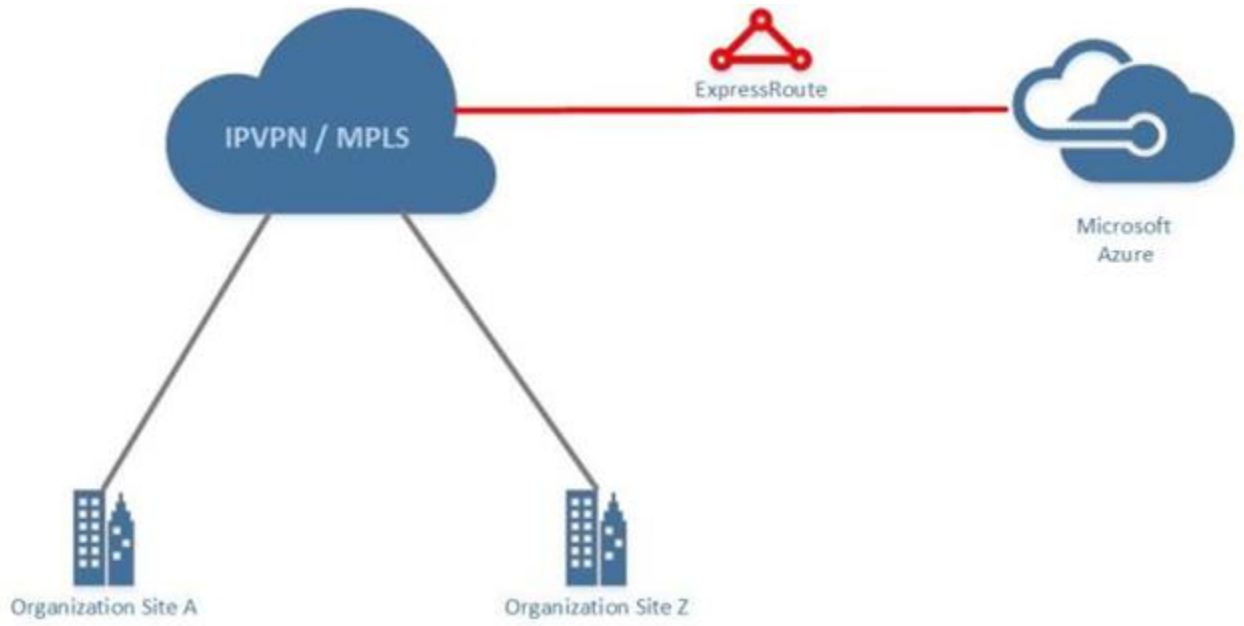
1. **Co-located at a cloud exchange.** If you are co-located in a facility with a cloud exchange, you can order virtual cross-connections to the Microsoft cloud through the co-location provider’s Ethernet exchange. Co-location providers can offer either Layer 2 cross-connections, or managed Layer 3 cross-connections between your infrastructure in the co-location facility and the Microsoft cloud.

2. **Point-to-point Ethernet connections.** You can connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. Point-to-point Ethernet providers can offer Layer 2 connections, or managed Layer 3 connections between your site and the Microsoft cloud.

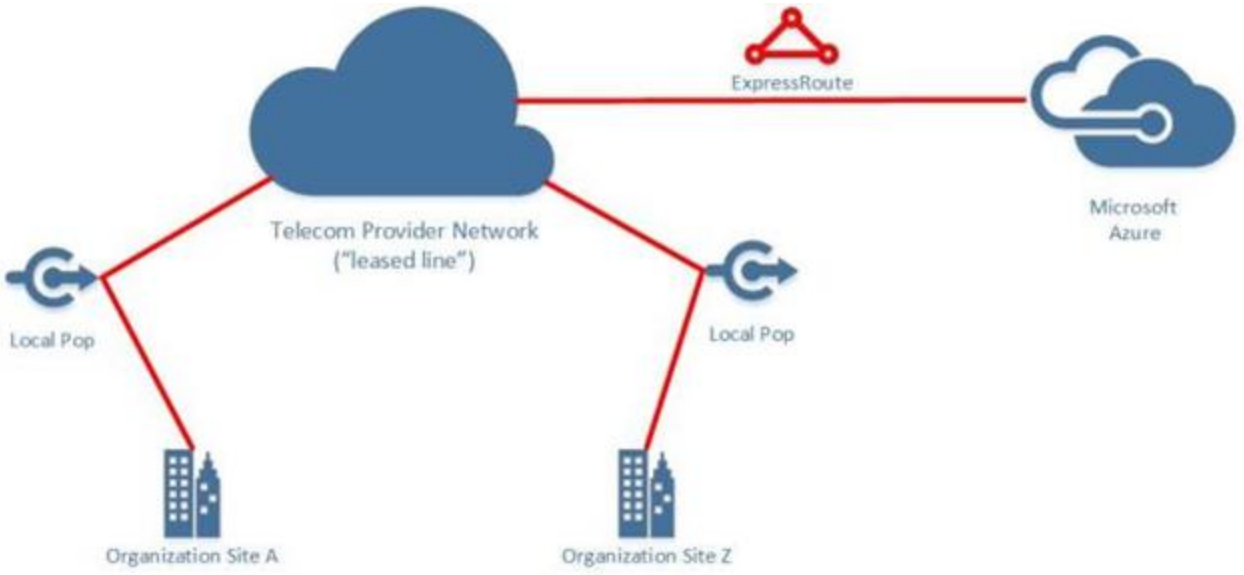
3. **Any-to-any (IPVPN) networks.** You can integrate your WAN with the Microsoft cloud. IPVPN providers (typically MPLS VPN) offer any-to-any connectivity between your branch offices and datacenters. The Microsoft cloud can be interconnected to your WAN to make it look just like any other branch office. WAN providers typically offer managed Layer 3 connectivity.

Explained Further

The “Any-to-Any”-connection is what used to be the “Network Service Provider” scenario. Here you add an “ExpressRoute” to your existing “IPVPN/MPLS” cloud / solution.



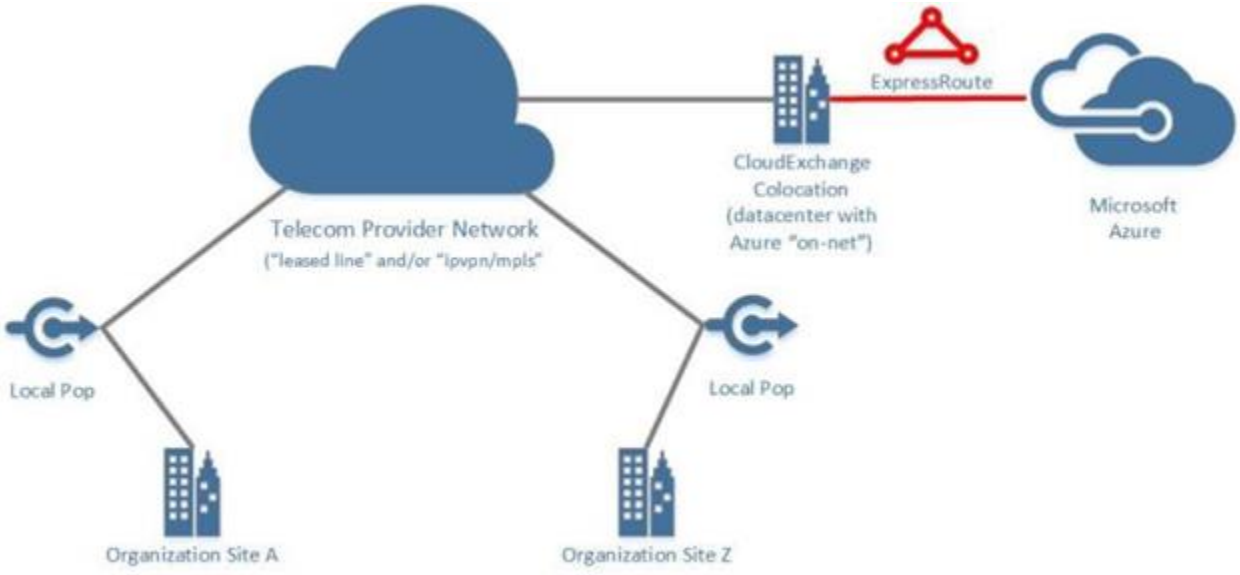
The **“Point-to-Point”-connection i**s what used to be the “Exchange Provider”-scenario. Here you get a direct connection from a Microsoft Azure Location to your own location. This location can be “On-Premise” or in a hosted datacenter.



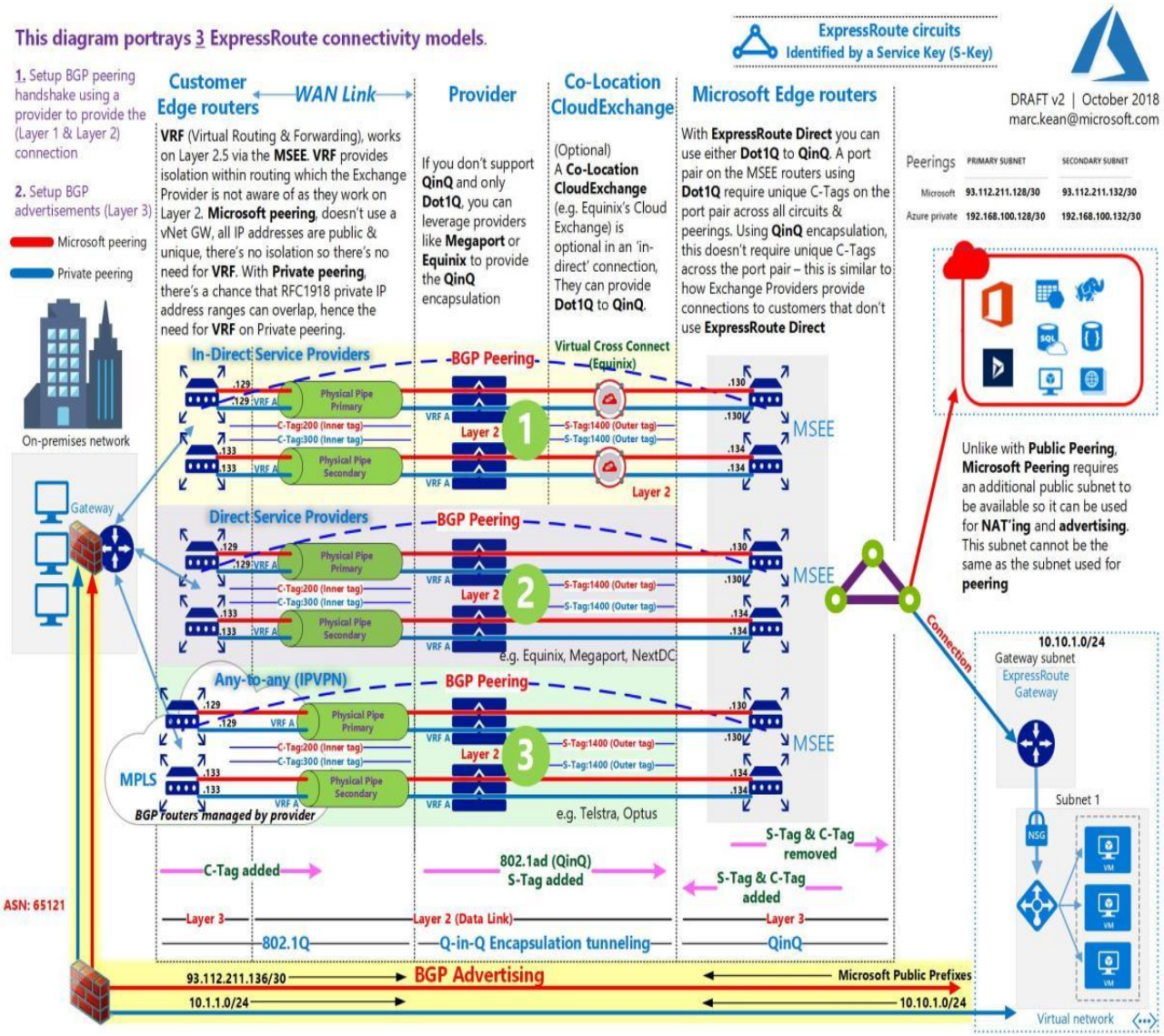
In the past, a complexity was also added with as there was a cost difference between a point-to-point connection to your On-premise/Hosted environment when compared to a datacenter which had “ExpressRoute” “On Net”. The “On Net” terminology is by telecom

& datacenter providers to indicate that there is no additional cost needed to provide the connectivity, as the datacenter is already foreseen with connectivity from the carrier.

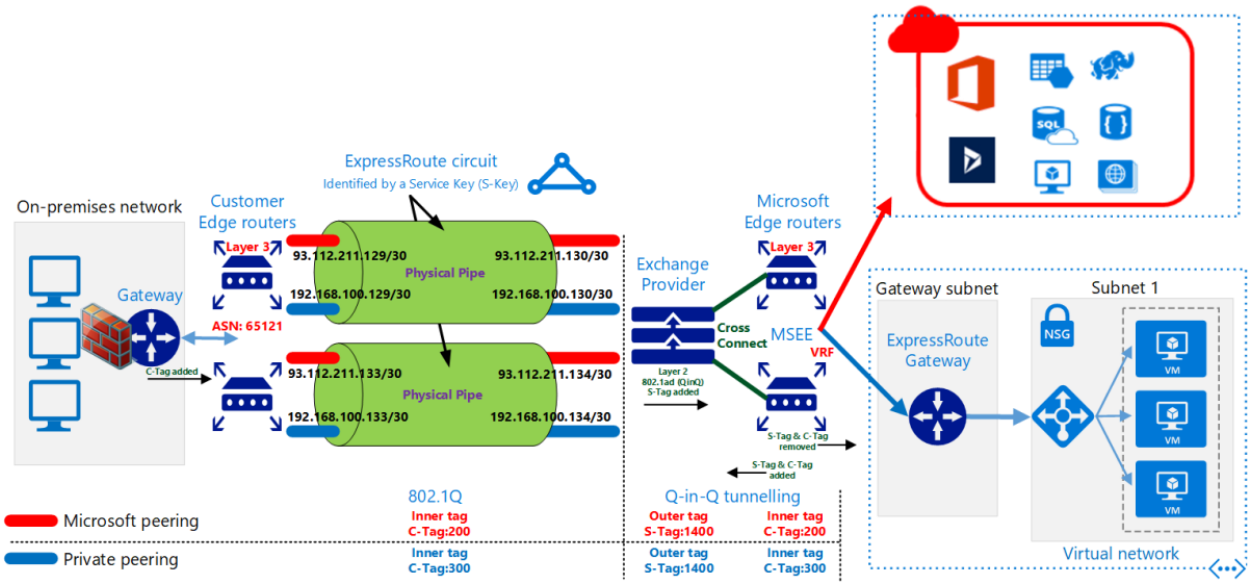
Here we notice that an additional naming has been introduced, being the “CloudExchange Colocation”. There are several datacenters which have been blessed with an “On Net” situation in regard to “ExpressRoute”.



If you split up ExpressRoute, customer on one side and Microsoft on the other side, the below segment has two parts in which it focuses on, the Microsoft side and the Customer side.

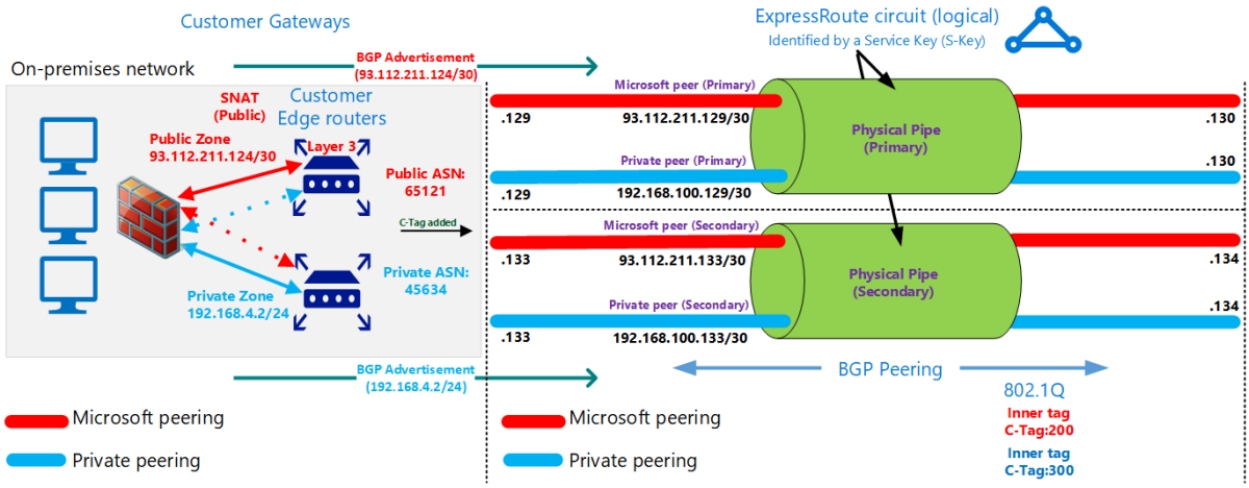


1. Microsoft side focus



- The C-Tag is different per peer type (Private/Microsoft). There are two C-Tags, one for Microsoft peering and one for Private peering. The C-Tag is used to identify the peer/routing domain. This tag is defined by customer and input in Azure Portal.
- The S-Tag has a one to one relationship with the ExpressRoute circuit, this applies to each circuit, an S-Tag for each circuit. This is defined by Microsoft and customer is not aware of it.
- For Microsoft peering, as there's no vNet gateway, it doesn't need isolation, as all IP addresses are public & unique, there is no need for VRF. The difference being, with private peering, there's a chance of an overlap of IP address ranges hence the need for VRF.
- VRF, works on Layer 2.5 at the MSEE level. VRF does isolation within routing, like a namespace in Linux. The Exchange Provider is not aware of VRF, because The Exchange Provider works on Layer 2, this is the maximum layer it can go to.
- Traffic to Azure | The Exchange Provider adds the S-Tag, then the MSEE removes both the S-Tag & C-Tag from the packet.
- Traffic from Azure | The MSEE adds both the S-Tag & C-Tag to the packet.
- The Exchange Provider equipment is a highly available layer 2 switch stack.
- Cross Connects are layer 1 physical connections between the Exchange Provider & the MSEE.

2. Customer side focus



- The BGP peers are setup independently as a first step prior to any NAT'ing & advertising of address ranges.
- Unlike with Public Peering, Microsoft Peering requires an additional public subnet to be available so it can be used for NAT'ing and advertising. This subnet cannot be the same as the subnet used for peering.
- Public IP addresses advertised to Microsoft over ExpressRoute must not be advertised to the Internet. This may break connectivity to other Microsoft services. However, Public IP addresses used by servers in your network that communicate with Office 365 endpoints within Microsoft may be advertised over ExpressRoute.
- With Microsoft peering, traffic destined to Microsoft cloud services must be SNATed to valid public IPv4 addresses before they enter the Microsoft network.

ExpressRoute Direct Model

Another way to create a connection between your on-premises network and the Microsoft cloud is via "Direct Model". In the ExpressRoute direct connectivity model (offered at 10/100 Gbps bandwidth), customers directly connect to Microsoft Enterprise Edge (MSEE) routers' port. Therefore, in the direct connectivity model, there are only customer and Microsoft network zones. The Microsoft Edge router is hosted on the Service Provider location. You don't use the Service Provider's network infrastructure, but you get authorization from Microsoft to hook up directly to their MSEE router ports.

Difference between ExpressRoute using a service provider and ExpressRoute Direct is provided in the link: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-erdirect-about#expressroute-using-a-service-provider-and-expressroute-direct

References:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-erdirect-about
Youtube:

1. ExpressRoute advanced - https://www.youtube.com/watch?v=0wsQrP6cAB8
2. ExpressRoute deep dive - https://www.youtube.com/watch?v=oevwZZ1YFS0

https://marckean.com/2018/09/03/azure-expressroute-demystified/
https://kvaes.wordpress.com/2016/02/10/azure-expressroute-connection-methods/
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-troubleshooting-expressroute-overview#overview