Module 3: Design and implement Azure ExpressRoute

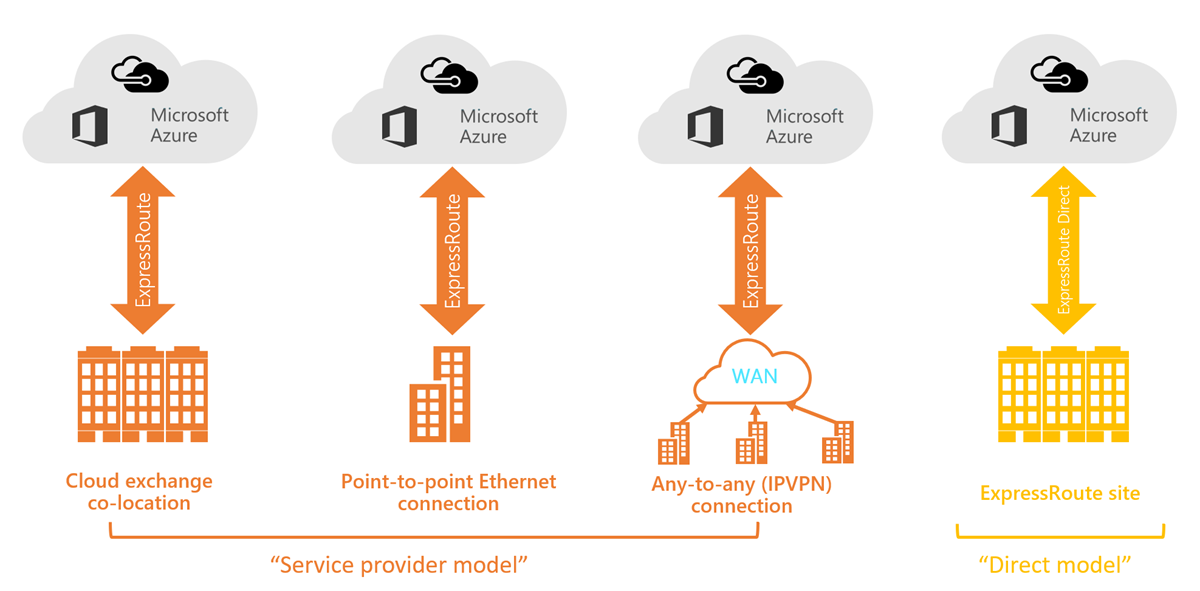
# Chapter 1: Explore Azure ExpressRoute

* ER extends on-prem networks into Azure cloud/365 over a private connection (not public Internet) w/ a connectivity provider.
  + Benefits:
    - Layer 3 connectivity between On-prem and Azure through a connectivity provider
    - Connectivity via:
      * Any-to-any (IPVPN) network
      * Point-to-point Ethernet connection
      * Virtual cross-connection via an Ethernet exchange
    - Connect to Azure cloud services across all regions in the geopolitical region
    - ER premium gives global connectivity to Azure services across all regions
    - Higher reliability w/ built-in redundancy in every peering location

## Use Cases for ER

* Faster and Reliable connection to Azure services via private connection
* Storage, backup, and Recovery
* Extend Data Centre capabilities to connect and add compute and storage capacity to existing data centres
* Predictable, reliable, and high-throughput connections

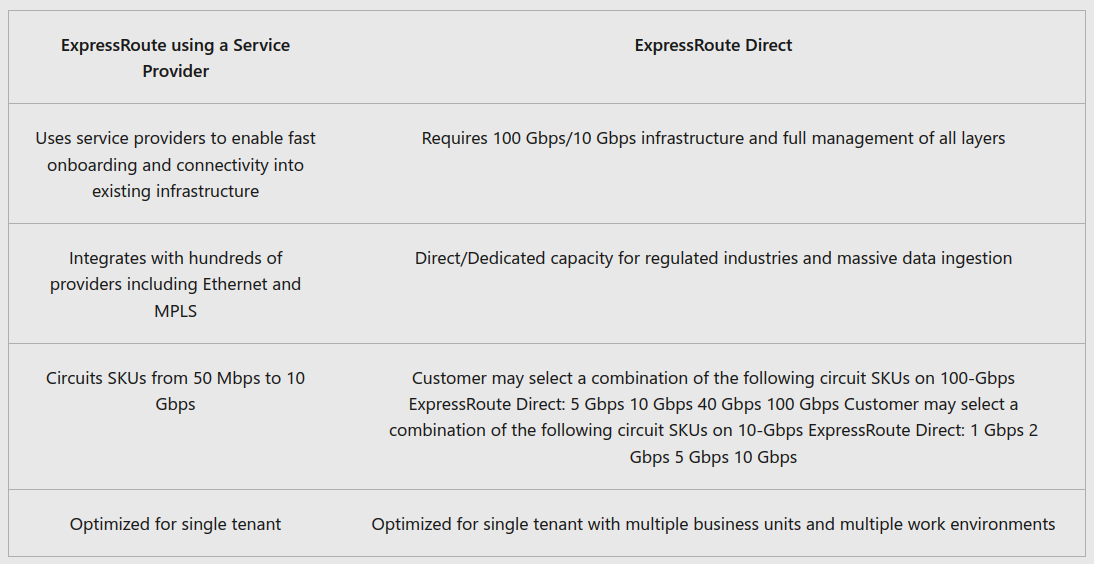
## ExpressRoute connectivity models



* CloudExchange Co-location
* Point-to-point Ethernet Connection
* Any-to-any (IPVPN) Connection (On-prem WAN w/ Azure cloud)
* ExpressRoute Direct (dual 100 Gbps or 10-Gbps connectivity)
  + Active/Active connectivity

## Design considerations for ExpressRoute deployments

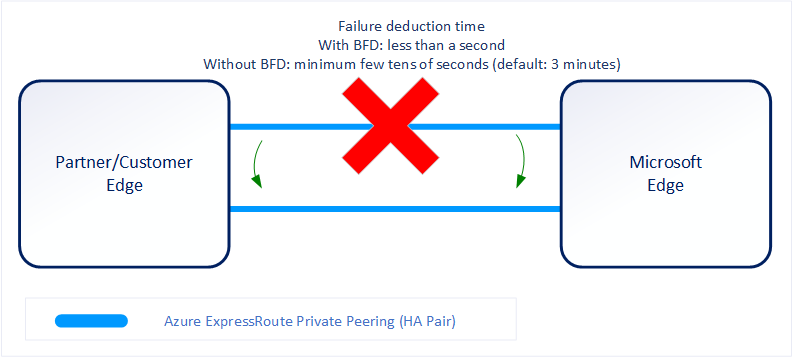
### Provider vs. Direct model

* **ER Direct**
  + Connect directly to MS global network peering locations (any service provider)
  + Benefits:
    - Data ingestion w/ Storage or Cosmos DB
    - Physical isolation/dedicated connectivity
    - Granular control of traffic
* **Comparison**
  + 

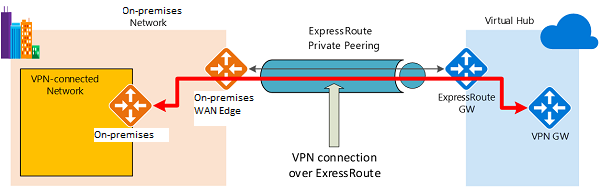
## Route Advertisement

* When initially peering on ER circuit, no routes are advertised to your network.
  + Use a route filter to enable route advertisements to your network:
    - Need active ER circuit w/ MS peering provisioned + enabled
    - Need a ER circuit enabled by connectivity provider
    - Either create MS peering yourself (you manage BGP session) OR Connectivity Provider provisions the peering

## Bidirectional Forwarding Detection (BFD)

* Can speed up “link failure detection” between MS Enterprise edge (MSEE) devices and the routers that your ExpressRoute circuit gets configured (CE/PE).
  + 
* BFD is configured by default under all the newly created ExpressRoute private peering interfaces on the MSEEs.
  + You must configure BFD on primary/secondary devices.
  + 1st time configuring peering on your ExpressRoute circuit, the Peerings are enabled by default.

## Configure encryption over ExpressRoute

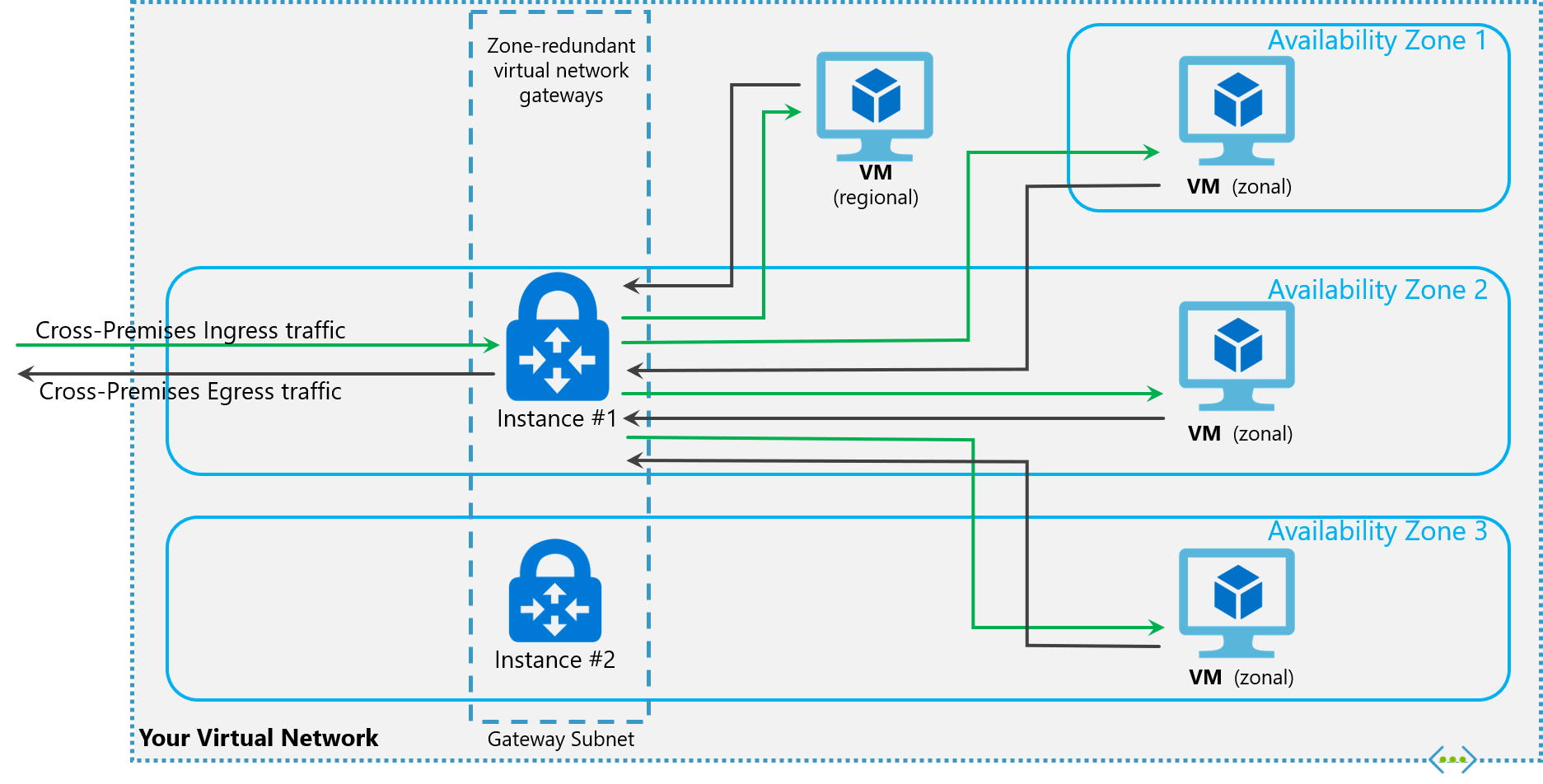
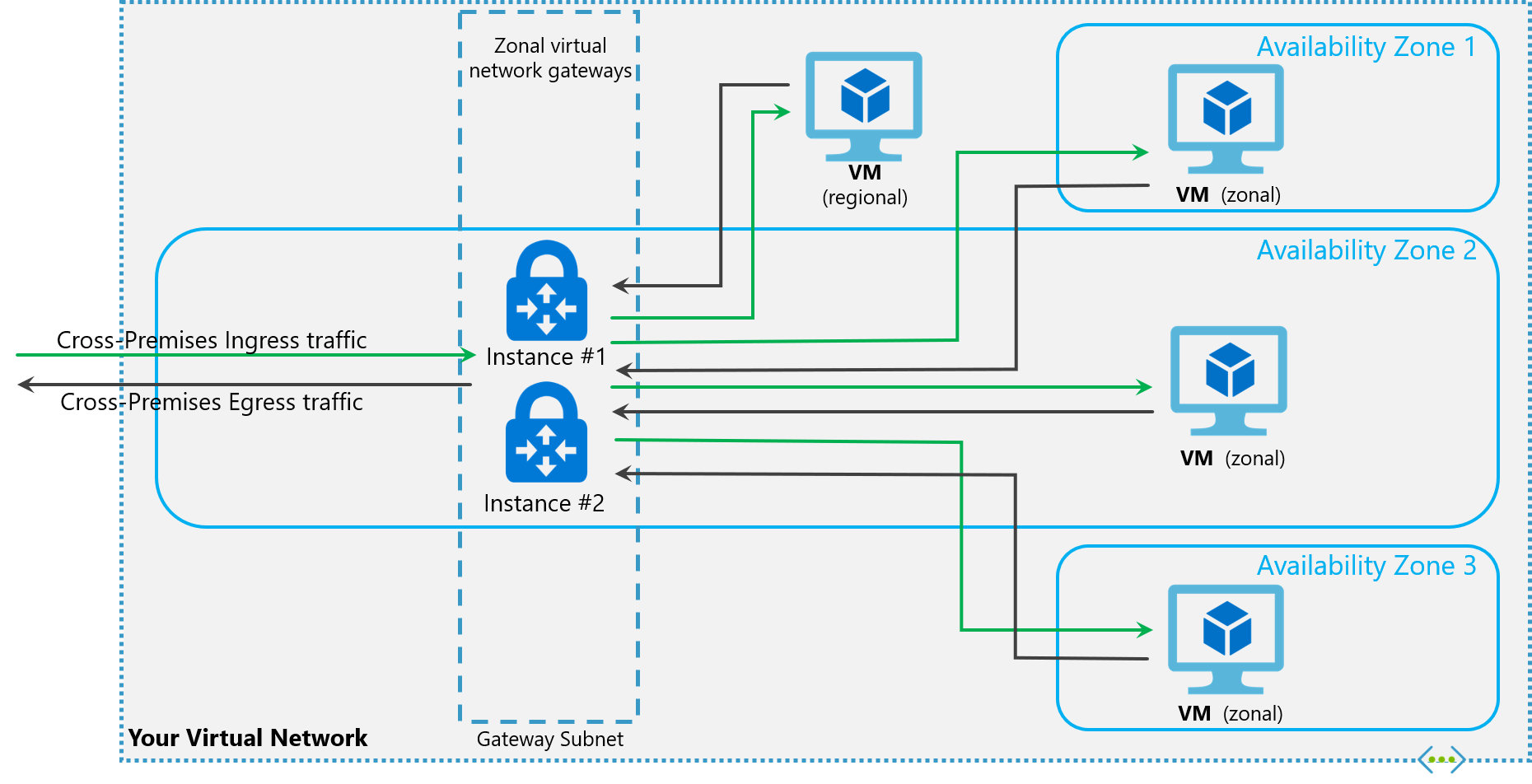
* Azure vWAN to establish VPN connection from on-premises to Azure over the private peering of ER circuit
  + **Topology/Routing of VPN connection over ER peering**
    - 
      * Establish ExpressRoute connectivity with an ExpressRoute circuit and private peering.
      * Establish the VPN connectivity.
  + **Traffic from on-premises networks to Azure**
    - Azure prefixes (VHUB and Spoke VNETS) are advertised via both the ER private peering BGP and the VPN BGP.
      * 2 Paths (on-prem to Azure):
        + One over the IPsec-protected path
        + One directly over ER w/o IPsec protection
  + **Traffic from Azure to on-premises networks**
    - 2 Options to ensure Ipsec path is used over direct ER path
      * Advertise more specific prefixes on the VPN BGP session for the VPN-connected network
      * Advertise disjoint prefixes for VPN and ExpressRoute.

## Design redundancy for an ER deployment (2 methods for redundancy)

### 1) Configure ExpressRoute and site to site coexisting connections

* **Benefits**:
  + Configure a S2S VPN as a secure fail-over path for ExpressRoute.
  + OR use S2S VPNs to connect to sites that are not connected through ExpressRoute.
* **Limitations**
  + Only route-based VPN gateway is supported.
  + The ASN of Azure VPN Gateway must be set to 65515.
  + The gateway subnet must be /27 or a shorter prefix, (such as /26, /25)
  + Coexistence in a dual stack VNET is not supported.

### 2) Create a zone redundant VNET gateway in Azure Availability zones

* Deploy VPN and ExpressRoute gateways in Azure Availability Zones.
  + **Zone-redundant gateways**
    - 
      * VNET gateways located across AZs (zone-resiliency)
  + **Zonal Gateways**
    - 
      * VNET gateways all in same AZs
* **Gateway SKUs**
  + Zone-redundant and zonal gateways are available as gateway SKUs.
    - You can identify these SKUs by the "AZ" in the SKU name.
* **Public IP SKUs**
  + Zone-redundant gateways and zonal gateways both rely on the Azure public IP resource **Standard** SKU.
    - Zone-redundant gateways
      * For a VPN gateway, the two gateway instances will be deployed in any **2 out of three** zones to provide zone-redundancy.
      * For an ExpressRoute gateway, the gateway can span across all the **three** zones.
    - Zonal gateways
      * All the gateway instances will be deployed in the same zone.
    - Regional gateways
      * Gateway is deployed as a regional gateway and does not have any zone-redundancy

# Chapter 3: Design Considerations for ER deployment

### ExpressRoute circuit SKUs

* **3 different circuit SKUs:** 
  + *Local SKU* - automatically charged with Unlimited data plan.
  + *Standard or Premium SKU* - Metered or an Unlimited data plan. All ingress data are free of charge except when using the Global Reach.

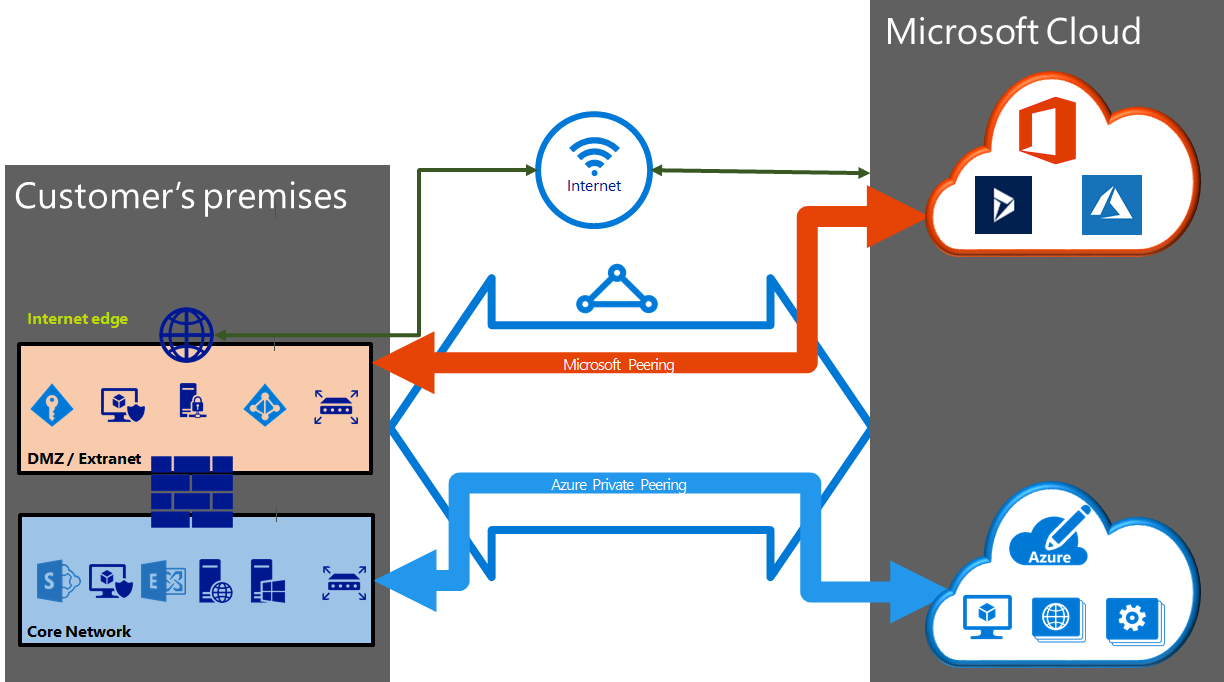
### Peering location

* Azure Region (determines datacentres & availability zones)
* ER locations (Peering locations)
  + They are co-location facilities where MS Enterprise Edge (MSEE) devices are located
  + Global distributed entry points to MS network
* Azure regions to ExpressRoute locations within a geopolitical region.
* ExpressRoute connectivity providers
* Connectivity through Exchange or Satellite providers
* National Research and Education networks (NERN)
* System integrators

### Choose the right ExpressRoute circuit and billing model

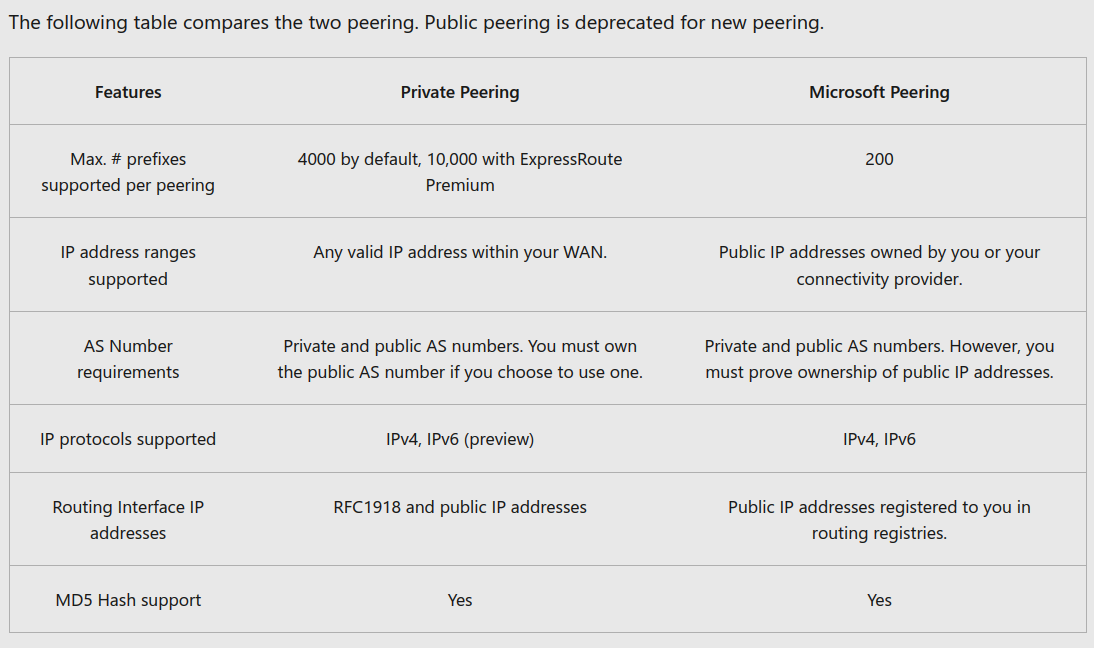
* Consider the **bandwidths** since ER circuit’s SKU type differ
* **Billing Model**
  + *Unlimited data*. (Billing is a monthly fee)
    - In/Outbound data transfer is free
  + *Metered data*. (Billing is a monthly fee)
    - Inbound data transfer is free
    - Outbound data transfer is charged per GB of data transfer.
  + *ExpressRoute premium Add-on for the ER circuit*.
    - **Capabilities**
      * Increased route limits for Azure public/Azure private peering from 4,000 to 10,000 routes.
      * Global connectivity for services.
        + ER circuit can access resources across every other region in the world.
      * Increased # of VNet links per circuit
        + 10 to a larger limit (bandwidth dependent).

# Chapter 6: Configure peering for an ExpressRoute deployment



* ER circuit peering options:
  + Azure private or Microsoft peering
  + **Create Peering configuration**
    - Need active ER circuit
    - When using shared key/MD5 hash, use key on both sides of tunnel
    - This only applies to Layer 2, but Layer 3 services are config/managed by connectivity provider

## Choose between private peering only, Microsoft peering only, or both

* 

### Private peering

* Used for VMs (IaaS) and cloud services (PaaS)
  + It is a trusted extension of core network in Azure
  + This peering connects to VMs and cloud services directly on their private IP addresses

### Microsoft peering

* Used for connecting to MS online services (Microsoft 365 and Azure PaaS services)
  + This peering connects you to MS cloud services via public IP (owned by you or connectivity provider)

### Route filters for Microsoft Peering

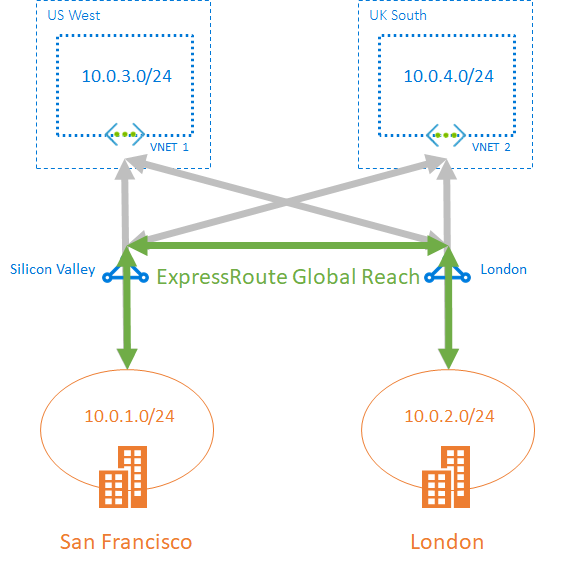
* Lets you consume a subset of supported services through Microsoft peering.
  + **Ex**. Microsoft 365 services (Exchange Online, SharePoint Online, and Skype for Business) are accessible through the Microsoft peering.
* Connectivity to all Azure and Microsoft 365 services causes many prefixes to gets advertised through BGP === many Route Tables created
  + Use Route Filters to:
    - Filter out unwanted prefixes by applying route filters on BGP communities.
    - Define route filters and apply them to your ExpressRoute circuit.
  + A route filter lets you identify services you want to consume through your ExpressRoute circuit's Microsoft peering
    - An allowed list of all the BGP community values.

# Chapter 7: Connect an ExpressRoute circuit to a virtual network

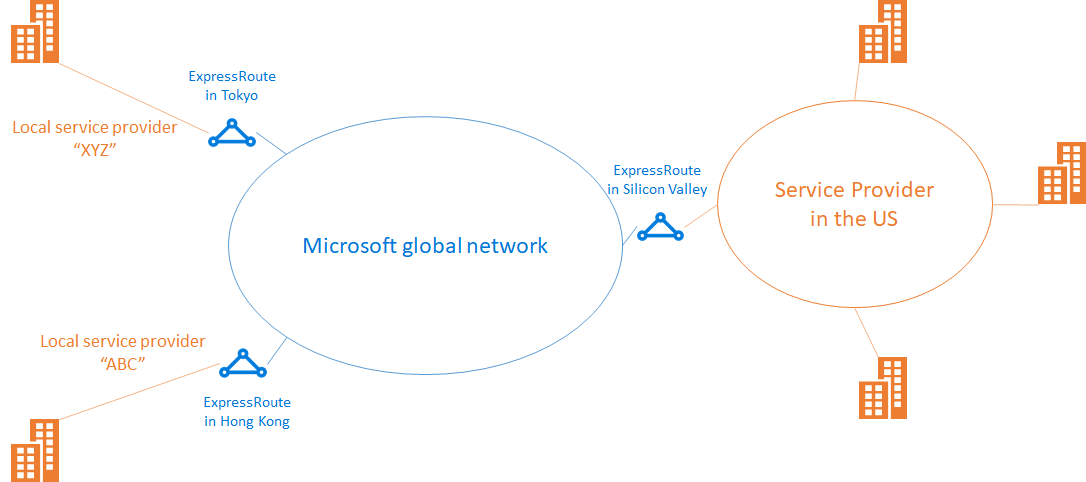
* Prerequisite to connect VNET to ER circuit
  + An active ExpressRoute circuit.
  + Ensure Azure private peering configured for circuit.
  + Azure private peering configured and establishes BGP peering between network and MS.
  + Ensure that there’s a VNET and VNET gateway created and fully provisioned ('ExpressRoute').
  + Link up to 10 VNETs to a standard ER circuit.
    - All VNETs must same geopolitical region
  + 1 VNET can be linked to 16 ER circuits.
  + ER premium add-on means you can link VNEts outside of the geopolitical region of the ER circuit + 10+ VNETs
  + Create a connection from ER circuit to the target ER VNET gateway
    - Need # of address spaces advertised from the local or peered VNETs <== 200.
    - Once successfully created, you can add additional address spaces, up to 1,000, to the local or peered VNET.

# Chapter 8: Connect geographically dispersed networks with ExpressRoute global reach

## Use cross-region connectivity to link multiple ExpressRoute locations

* Methods for region connectivity:
  + Connect to all regions *within a geopolitical region*
    - Connect to MS in one peering location to access regions within the geopolitical region.
    - **Ex**. Connect in MS Amsterdam via ER, you can access to all MS cloud services hosted in Northern and Western Europe.
  + *Global connectivity* with ER Premium
  + *Local connectivity* with ER Local
    - Enable the Local SKU to bring your data to ER location near the Azure region you want.
  + *Across on-premises connectivity* with ER Global Reach
  + Rich *connectivity partner* ecosystem
  + Connectivity to *national clouds*
    - Special isolated cloud environments for special geopolitical regions and customer segments.
  + *ExpressRoute Direct*
    - Connect directly into MS global network at peering locations distributed across the world
    - 

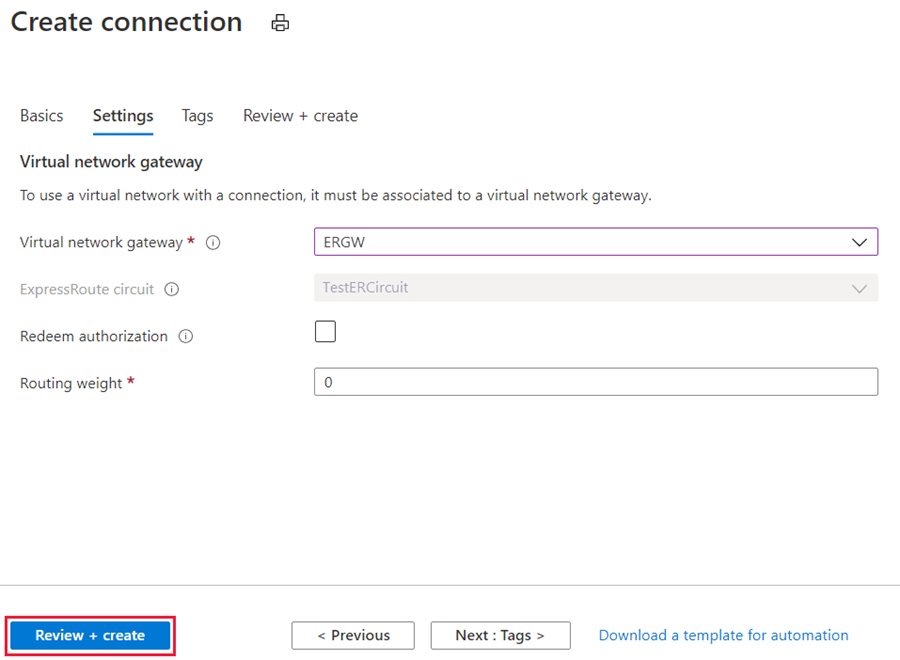
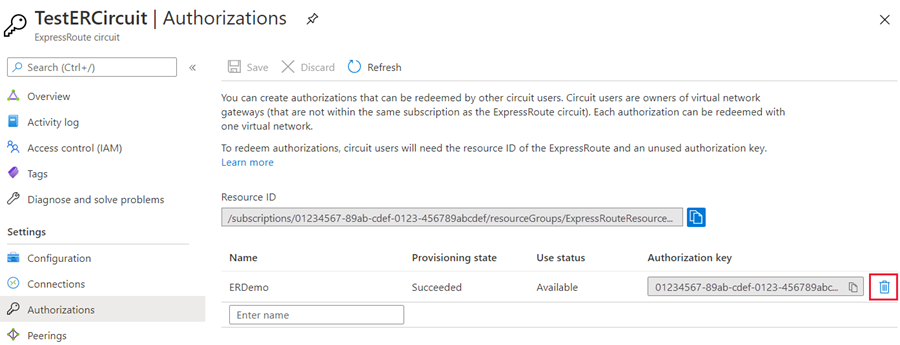
## When to use ER global reach

* Complements your service provider’s WAN implementation and connects your **branch offices** across the world.
  + 

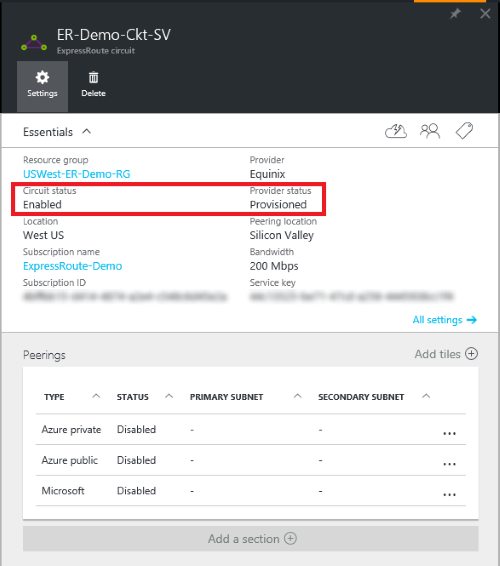
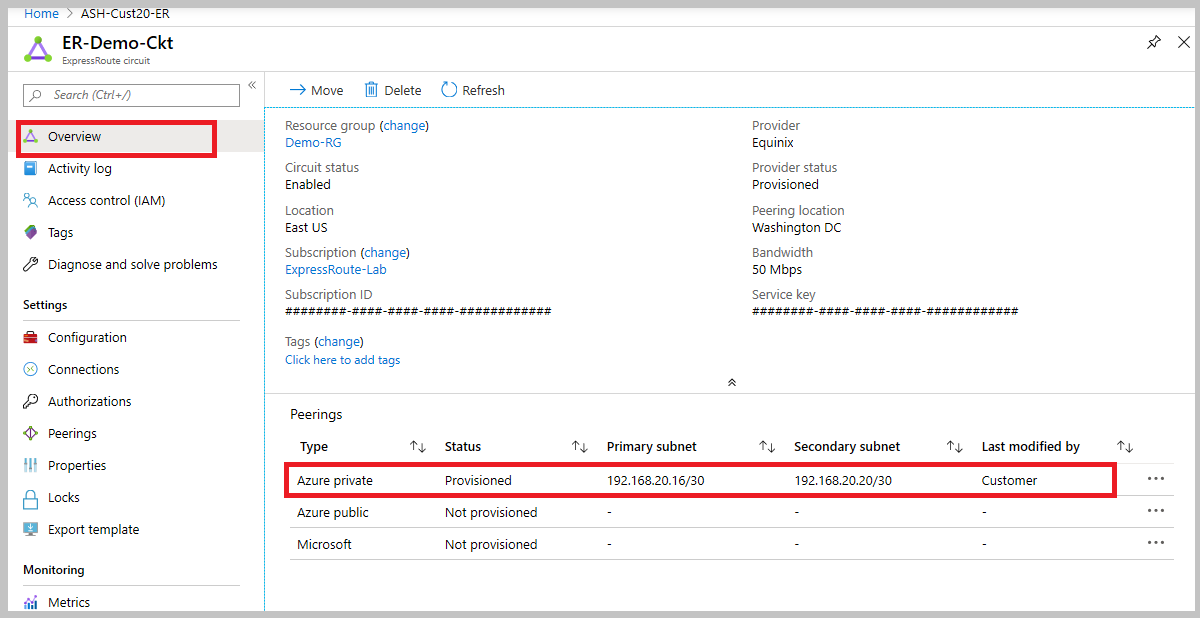
# Chapter 9: Improve data path performance between networks with ExpressRoute FastPath

* FastPath improves data path performance between on-premises and Azure VNET.
  + It sends network traffic directly to VMs in VNET, bypassing the gateway.
    - It still requires a VNET gateway to exchange routes between On-prem and Az VNET
    - Gateway must be either: Ultra-Performance OR ErGw3AZ (IPv6 private peering req.)
* **Limitations (does not support):**
  + *UDR on the gateway subnet* has no impact on the network traffic sent by FastPath
  + VNET Peering
  + Basic Load Balancer
  + Private Link/private endpoint
    - Connection will go through the VNET gateway.

## Configure ER FastPath

* Connect a VNet to a circuit - same subscription
  + 
* **Administration** - circuit owners/users
  + Owner is an authorized Power User of the ExpressRoute circuit resource.
    - Owner creates authorizations that can be redeemed by 'users'.
    - Users own VNET gateways that are not within the same subscription as the ExpressRoute circuit. They redeem authorizations (one per VNEt ).
  + Owner modify/revoke authorizations at any time.
  + 

# Chapter 10: Troubleshoot ExpressRoute connection issues

* **Verify circuit provisioning and state through the Azure portal**
  + ER circuit is operational when: the Circuit status = Enabled, and Provider status = Provisioned.
    - 
      * Circuit status == status of the circuit on MS side.
      * Provider status === Provisioned/Not provisioned the service-provider side.
* **Validate peering configuration**
  + ****
    - A successfully provisioned peering context would have the **primary and secondary** point-to-point subnets listed.
* **Validate Address Resolution Protocol (ARP)**
  + ARP is a layer 2 protocol defined in RFC 826 used to map the Ethernet address (MAC address) with an IP address.
    - Can be used to troubleshoot/validate basic layer 2 connection issues
  + No ARP table for MS side, only on user side
    - Open Support ticket for assistance
* **ExpressRoute monitoring tools**
  + Analyze metrics for Azure ER with metrics from other Azure services using **metrics explorer** in Azure Monitor menu.