Azure Talk – Azure Networking

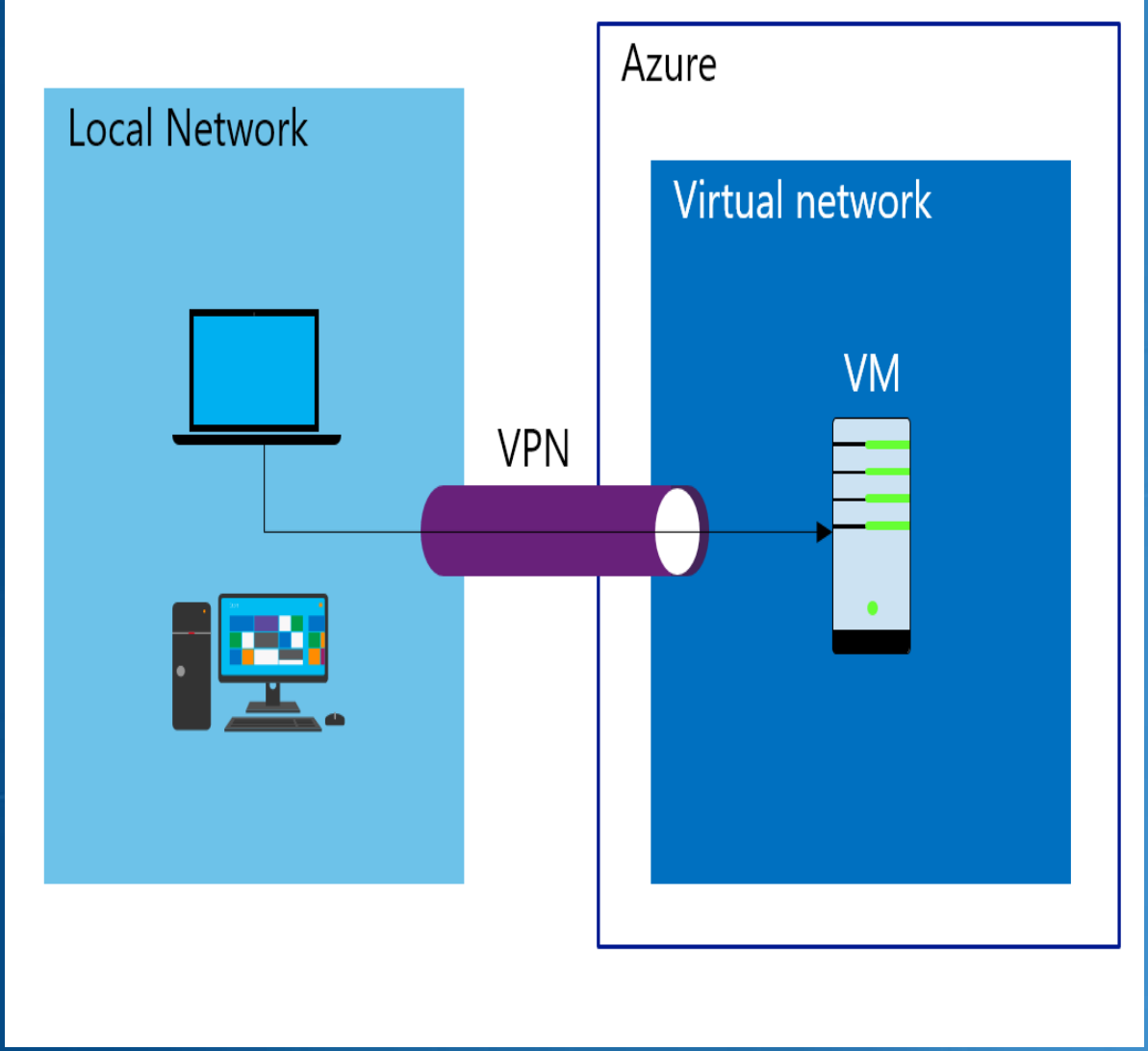
Niraj Kumar
Cloud Architect, MCT(Microsoft Certified Trainer)

Agenda

Azure Networking

- Vnet (Virtual Network)
- Subnets
- CIDR Block
- IP Addresses
- NSG (Network Security Group)
- On-Premise network connectivity
  - VPN
  - ExpressRoute
- NIC
- Azure Load Balancer (Internal and Internet)
- DNS
- Application Gateway (Layer 7 and WAF)
- Traffic Manager
- UDR (User Defined route)
- Forced Tunneling

Azure Networking, Vnet, Subnet and CIDR block.



- Azure **Virtual Network** is a fundamental component that acts as an organization's network in Azure.
- It defines an organization's network in the cloud, where the administrators can have full control over IP address assignments, name resolution, security settings, and routing rules.
- When a VNET is created you define the scope of IP addresses. These three address spaces are the only ones that are supported within an Azure VNet. The address spaces are:·
  - 10.0.0.0/8 -> 10.0.0.1 to 10.255.255.255
  - 172.16.0.0/12 -> 172.16.0.1 to 172.31.255.255
  - 192.168.0.0/16 -> 192.168.0.1 to 192.168.255.255

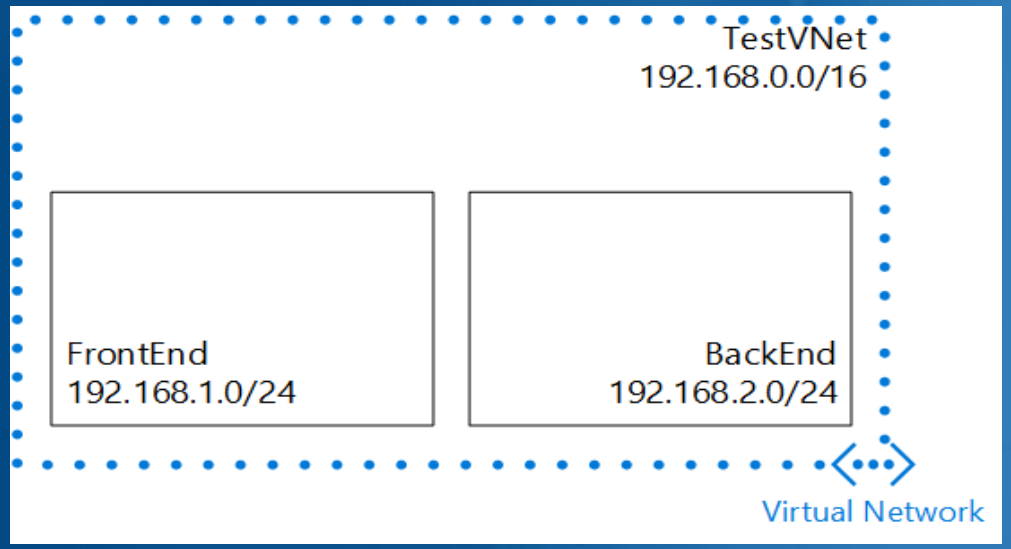
Azure Networking, Subnet , CIDR and IP addreses.

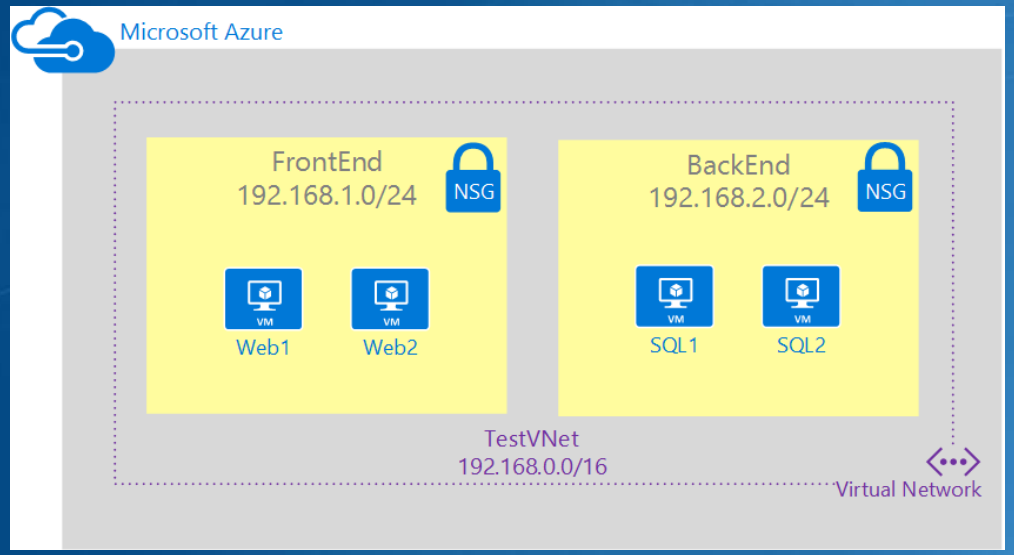
- **Subnet**
  - A **subnet** is a range of IP addresses in the VNet. You can divide a VNet into multiple subnets.
  - VMs deployed to subnets (same or different) within a VNet can communicate with each other without any extra configuration.
  - You can also configure route tables and NSGs to a subnet.
  - Within each subnet, the first three IP addresses and the last IP address are reserved and cannot be used for VMs. The smallest subnets that are supported use a 29 bit subnet mask.
- **CIDR**
  - CIDR is a way to represent network IP block. The length of the network prefix in IPv4 CIDR is specified as part of the IP address.
  - For example: 192.30.250.0/24 The "192.30.250.0" is the network address itself and the “24" says that the first 24 bits are the network part of the address, leaving the last 8 bits for specific host addresses.
- **IP Addresses:** There are two types of IP addresses you can use in Azure:
  - Public IP addresses: Used for communication with the Internet, including Azure public-facing services. It can be either static or dynamic and are assigned to VM, Internet-facing load balancers, VPN gateways and Application gateways
  - Private IP addresses: Used for communication within an Azure virtual network (VNet), and your on-premises network. It can be set dynamic(DHCP lease) or static(DHCP reservation).

Azure Networking, NSG (Network Security Group)

- **Network Security Group** provides advanced security protection for the VMs that you create in Azure.
- It controls inbound and outbound traffic passing through a Network Interface Card (NIC) (Resource Manage deployment model), a VM (classic deployment), or a subnet (both deployment models).
- **Network Security Group rules** specify whether the traffic is approved or denied. Each rule consists of the following properties:
  - Name: A unique identifier for the rule.
  - Direction: Traffic is inbound or outbound.
  - Priority: Rules with higher priority apply.
  - Access: Specifies whether the traffic is allowed or denied.
  - Source IP address prefix: This identifies from where traffic originates.
  - Source port range: This specifies source ports.
  - Destination IP address prefix: This identifies the traffic destination
  - Destination port range: This specifies destination ports
  - Protocol: Protocol specifies a protocol that matches the rule. It can be UDP, TCP, or the asterisk (*) wildcard character *.

Azure Networking, NSG (Network Security Group)



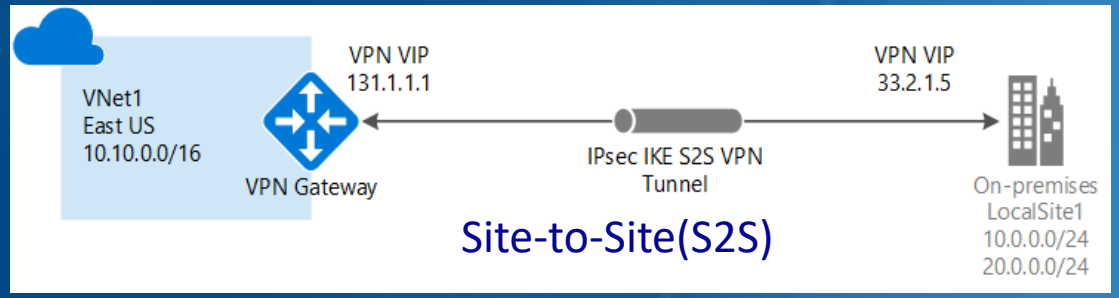


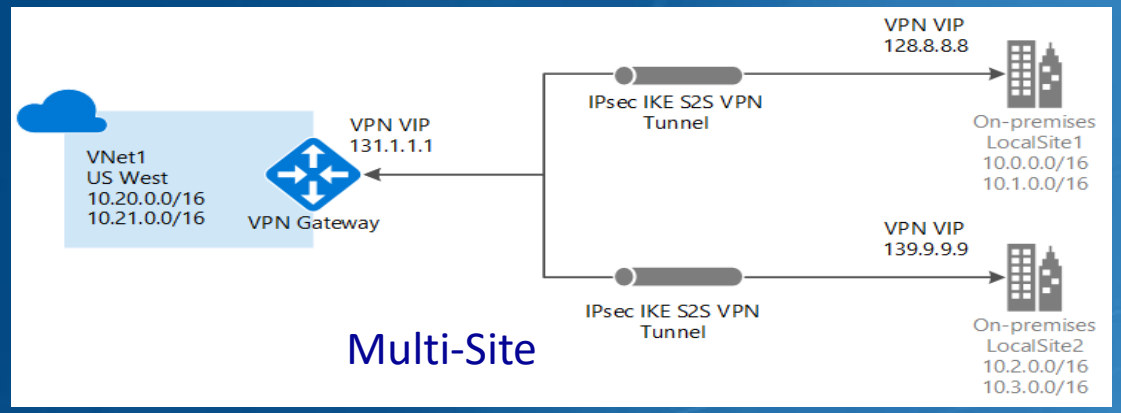
- NSG-FrontEnd.
  - rdp-rule. This rule will allow RDP traffic to the FrontEnd subnet.
  - web-rule. This rule will allow HTTP traffic to the FrontEnd subnet.
- NSG-BackEnd.
  - sql-rule. This rule allows SQL traffic only from the FrontEnd subnet.
  - web-rule. This rule denies all internet bound traffic from the BackEnd subnet.

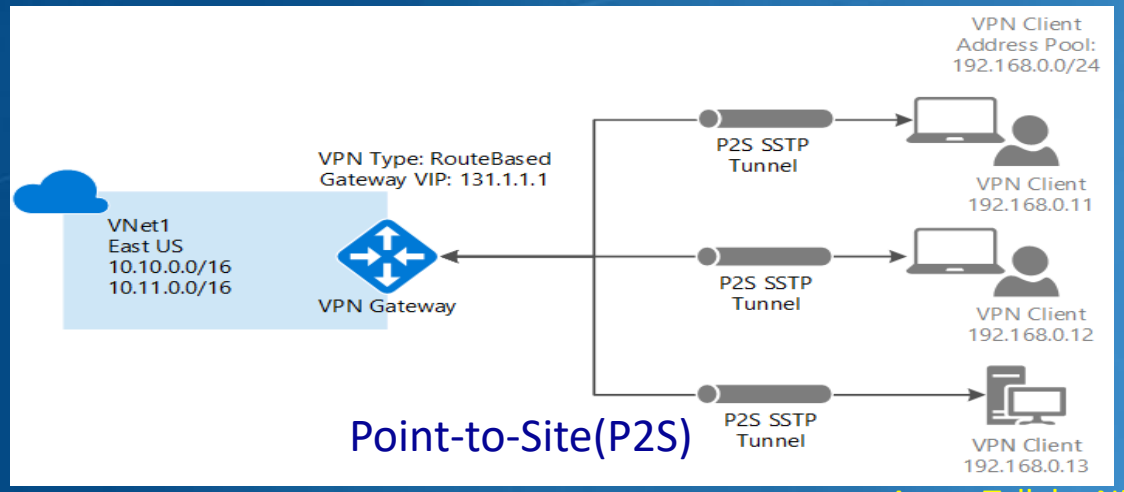
Azure Networking, On-Premise Network connectivity

- Virtual networks enable you to extend your on-premises networks to the cloud.
- You can enable on-premises users to access Azure services as if they were physically located on-premises in your own datacenter.
- To connect to an Azure virtual network from an on-premises network, you can use:
  - Point-to-Site VPN
  - Site-to-Site VPN
  - Multi-Site VPN
  - VNet-to-VNet
    - S2S VPN
    - Vnet Peering
  - ExpressRoute

Azure Networking, VPN Gateway

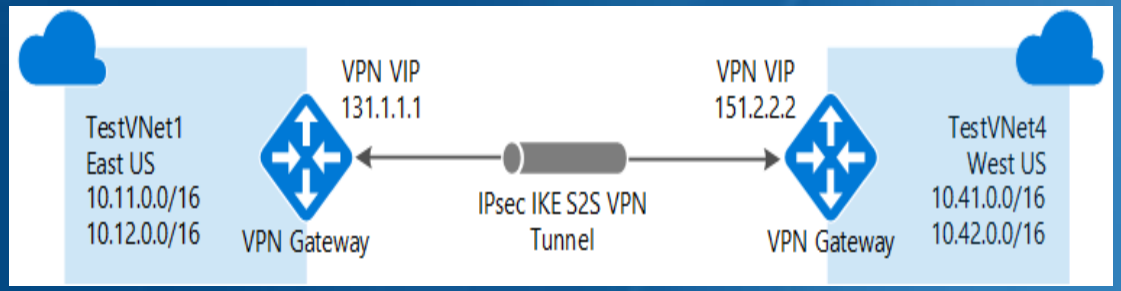


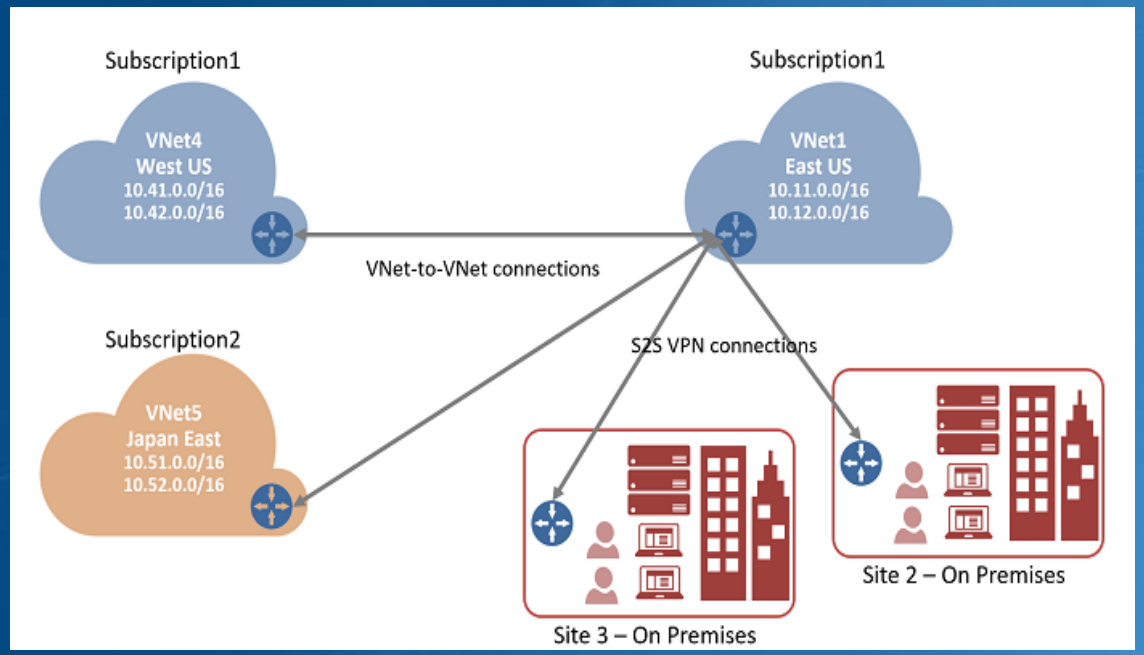




- A **VPN gateway** is a type of virtual network gateway that sends encrypted traffic across a public connection to an on-premises location or to an Azure virtual networks over the Microsoft network.
- Each virtual network can have only one VPN gateway, however, you can create multiple connections to the same VPN gateway.
- Connection topology
  - **Site-to-Site:** A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.
  - **Multi-Site:** You create more than one VPN connection from your virtual network gateway, typically connecting to multiple on-premises sites. When working with multiple connections, you must use a RouteBased VPN type.
  - **Point-to-Site:** A P2S connection allows you to create a secure connection to your virtual network from an individual client computer.
  - **Vnet-to-Vnet:** Connecting a virtual network to another virtual network (VNet-to-VNet) is similar to connecting a VNet to an on-premises site location.
  - **Vnet Peering:** Virtual network peering enables you to connect two virtual networks in the same region through the Azure backbone network. It doesn't require use of VPN gateway.

Azure Networking, VPN Gateway and Vnet peering



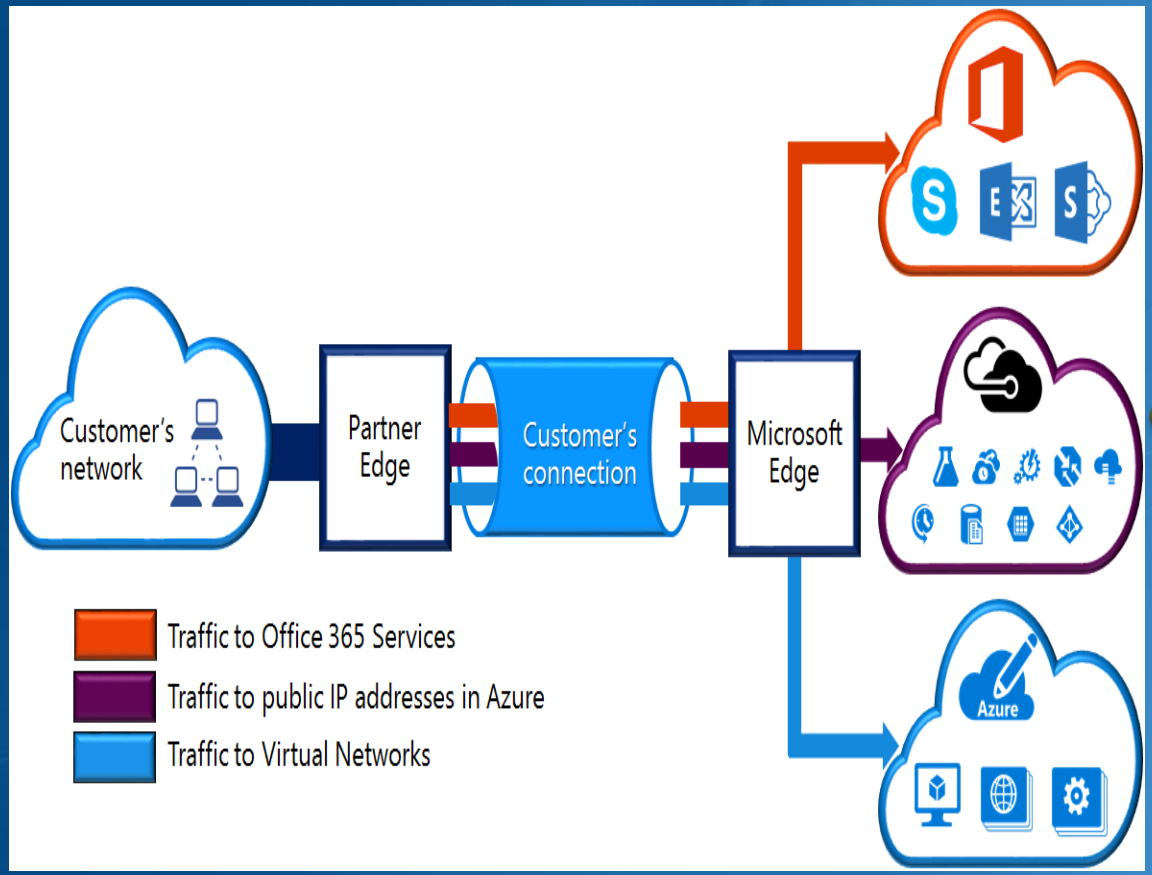


- Create and configure Vnets
- Add additional address space and create subnets
- Create a gateway subnet
- Create a virtual network gateway
- Configure VPN connection.
- Verify Vnet connectivity
- Configure Vnet Peering with remote gateway

VPN gateway and Vnet peering Configuration

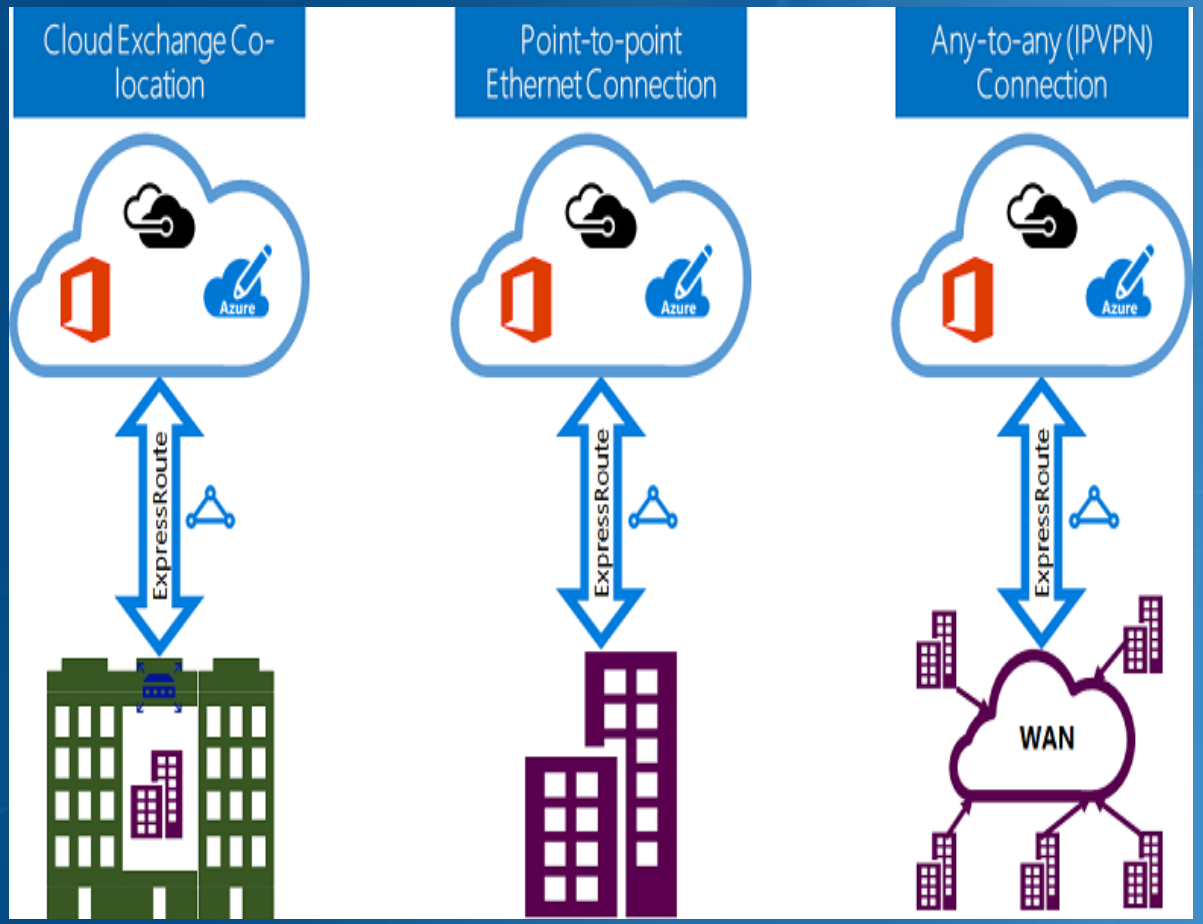
Niraj Kumar
Cloud Architect

ExpressRoute



- What is **ExpressRoute**?
  - ExpressRoute enables you to establish a *dedicated private, reliable, high speed connectivity* between your data center and Microsoft Azure.
  - ExpressRoute circuit is isolated using *industry standard VLANs* to allow private, secure access to resources deployed in Microsoft Azure Virtual Networks.
- Benefits of ExpressRoute
  - **Network Privacy**
  - Hybrid Applications
  - Cross Region Connectivity with premium addon.
  - Predictable Network Performance
  - Built-in redundancy in every peering location for higher reliability.
  - Dynamic routing between your network and Microsoft over BGP.

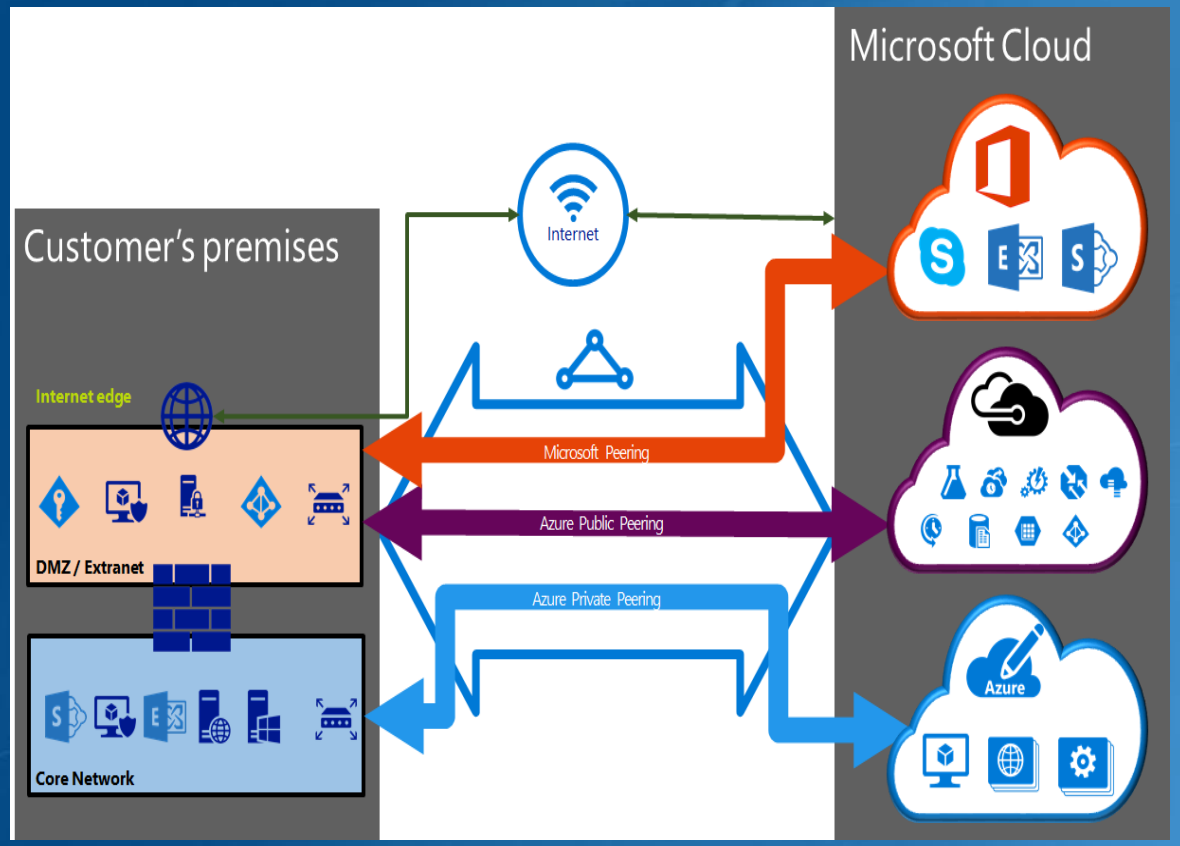
ExpressRoute Connectivity Model



Express route offers three connectivity Model:

- **Co-located at a cloud exchange**: 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. Layer 2 or Layer 3.
- **Point-to-point Ethernet connections**: You can connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. Layer 2 or Layer 3.
- **Any-to-any (IPVPN) networks**: You can integrate your WAN with the Microsoft cloud. The Microsoft cloud can be interconnected to your WAN to make it look just like any other branch office.

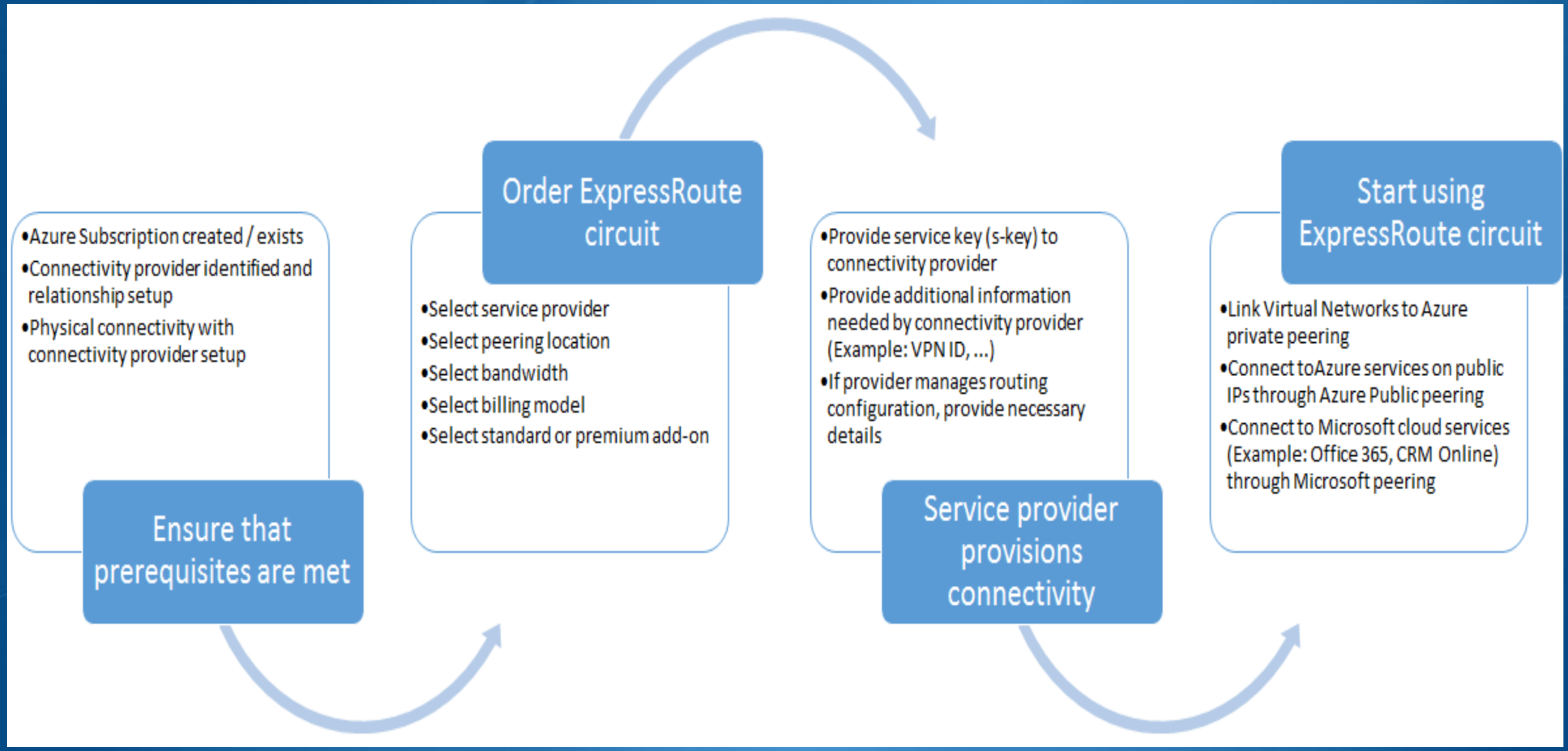
ExpressRoute Routing Domain



ExpressRoute circuits do not map to any physical entities. A circuit is uniquely identified by a standard GUID called as a service key (s-key). An ExpressRoute circuit can have up to three independent peerings:

- **Private peering**: This peering lets you connect to virtual machines and cloud services directly on their private IP addresses.
- **Public peering:** Services such as Azure Storage, SQL databases, and Websites are offered on public IP addresses. You can privately connect to services hosted on public IP addresses. Microsoft doesn't allow you to selectively pick services for which you want to enable public peering.
- **Microsoft peering:** It offers connectivity to Microsoft SaaS like Office 365 and Dynamic CRM.

ExpressRoute provisioning workflow



ExpressRoute creation and configuration

demo

Niraj Kumar
Cloud Architect, MCT