**Handout: Administer Intersite Connectivity**

**1. What is Intersite Connectivity?**

Intersite connectivity refers to the **connection between different virtual networks (VNets)**, regions, and even on-premises data centers. Azure provides multiple ways to securely and efficiently connect these networks to ensure seamless communication and data transfer.

**2. Virtual Network Peering**

* **What is VNet Peering?**  
  VNet peering connects two Azure virtual networks, allowing resources in both VNets to communicate with each other using **private IP addresses**.
* **Types of VNet Peering**:
  + **Global Peering**: Connects VNets across different regions.
  + **Regional Peering**: Connects VNets within the same region.
* **Advantages of VNet Peering**:
  + Uses Azure’s backbone network, ensuring **high-speed**, **low-latency**, and **secure** connections.
  + VNets can span across subscriptions or even tenants, making it flexible for large organizations.
* **Gateway Transit**:  
  Allows peered virtual networks to share a single **VPN Gateway** for external connectivity, reducing costs and simplifying management.
* **Service Chaining**:  
  You can direct traffic between VNets via a **virtual appliance** (e.g., firewall, VPN gateway) to implement custom routing and security measures.

**3. VPN Gateway**

* **What is a VPN Gateway?**  
  VPN Gateway provides **secure communication** between Azure and on-premises networks or between different Azure VNets using **IPsec/IKE protocols**.
* **VPN Gateway Use Cases**:
  + **VNet-to-VNet Connections**: Establishes a secure tunnel between VNets in Azure.
  + **Site-to-Site VPN Connections**: Connects your on-premises data center to Azure, allowing for a **hybrid cloud** environment.
  + **Point-to-Site VPN Connections**: Allows individual devices to securely connect to Azure resources.
* **Gateway Subnet**:  
  When setting up a VPN gateway, a dedicated **gateway subnet** is required to host the gateway resources. No other resources should be deployed in this subnet.
* **High Availability Scenarios**:
  + **Active/Standby**: Two VPN gateway instances ensure redundancy, where only one is active at a time.
  + **Active/Active**: Both VPN gateway instances are active, providing higher availability and load balancing.

**4. ExpressRoute**

* **What is ExpressRoute?**  
  ExpressRoute provides a **dedicated, private connection** between your on-premises network and Azure. Unlike VPNs, it does not route traffic over the public internet, offering enhanced security, reliability, and **low-latency** communication.
* **Key Features of ExpressRoute**:
  + **Private Connections**: Data travels directly between your data center and Azure without touching the internet.
  + **High Throughput**: Supports speeds from **50 Mbps to 100 Gbps**, ideal for large data transfers or latency-sensitive applications.
  + **Global Connectivity**: With the ExpressRoute **Premium Add-on**, you can connect across different regions and enable global reach for your workloads.
* **ExpressRoute and VPN Coexistence**:  
  ExpressRoute can coexist with Site-to-Site VPN as a failover option. For example, if the ExpressRoute connection fails, traffic can be rerouted through the VPN.

**5. Azure Virtual WAN (VWAN)**

* **What is Virtual WAN?**  
  Azure Virtual WAN brings together various types of network connections, such as **Site-to-Site (S2S), Point-to-Site (P2S)**, and **ExpressRoute**, into a centralized, managed hub.
* **VWAN Features**:
  + **Integrated Hub-and-Spoke Model**: VNets and on-premises locations connect to a central hub, enabling simplified routing and security management.
  + **End-to-End Connectivity Visualization**: You can visualize and manage the flow of traffic across your Azure environment, enhancing your control over network topology.
  + **Global Reach**: Virtual WAN enables global network connectivity across Azure regions.

**6. Lab 05: Implement Intersite Connectivity**

* **Lab Scenario**:  
  In this lab, you will simulate Contoso's on-premises network setup, with datacenters in Boston, New York, and Seattle. The goal is to replicate the **topology of the on-premises network** using Azure resources and ensure full connectivity between the VNets.
* **Objectives**:
  + **Task 1**: Provision the lab environment with multiple VNets.
  + **Task 2**: Configure both local and global **VNet Peering** to establish communication between VNets.
  + **Task 3**: Test the **intersite connectivity** to ensure that resources in the VNets can communicate seamlessly.

**7. Comparison of Intersite Connectivity Options**

* **VNet Peering vs. VPN Gateway vs. ExpressRoute**:
  + **VNet Peering**: Best for low-latency, high-bandwidth communication between Azure VNets.
  + **VPN Gateway**: Ideal for secure communication between Azure and on-premises networks.
  + **ExpressRoute**: Provides a private, dedicated connection for enterprises needing high performance and secure communication without using the public internet.

**8. Knowledge Check**

* **Q1**: What are the advantages of using **VNet Peering** over VPN Gateway?
* **Q2**: How does **Gateway Transit** simplify the setup of multiple VNets?
* **Q3**: Explain two high-availability options for VPN Gateways.
* **Q4**: What are three key features of **Azure ExpressRoute**?
* **Q5**: How does **Azure Virtual WAN** simplify network connectivity in Azure?