**Question 2: What are the key considerations and limitations when setting up VNet Peering between two virtual networks?**

Ans:-

**CONSIDERATIONS:**

1. **Virtual** **networks in the same region:** VNet Peering can only be established between virtual networks in the same region.
2. **Virtual networks in different subscriptions:** VNet Peering can be established between virtual networks in different subscriptions, but both subscriptions must be associated with the same Azure Active Directory tenant.
3. **Peering must be created from both virtual networks:** Peering connections need to be created from both virtual networks to establish a bi-directional communication link.
4. **Security rules:** Traffic between peered virtual networks is subject to security rules configured on the subnets and the network interfaces.
5. **Global VNet Peering:** Global VNet Peering is available for virtual networks in different regions, but it has some limitations compared to regional peering.
6. **Peering state:** Peering connections can be in different states, such as Connected, Disconnected, Initiated, or Invalid. It's important to monitor the peering state to ensure that the communication link is working as expected.

**LIMITATIONS:**

1. **No transitive peering:** Peering connections are not transitive. If virtual network A is peered with virtual network B, and virtual network B is peered with virtual network C, virtual network A is not automatically peered with virtual network C.
2. **Scale limitations:** There are some scale limitations for VNet Peering. For example, you can have up to 100 peering connections per virtual network, and up to 5000 total peering connections per subscription.
3. **Firewall rules:** Firewall rules applied to a subnet in one virtual network do not affect traffic to peered virtual networks.
4. **Virtual network gateways**: Virtual network gateways cannot be used with VNet Peering. If you need to connect virtual networks across regions or connect on-premises networks to Azure, you should use VPN Gateway or ExpressRoute instead.
5. **Private IPv6 traffic:** Global VNet Peering does not support private IPv6 traffic.
6. **Higher latency:** Global VNet Peering has higher latency compared to regional peering.