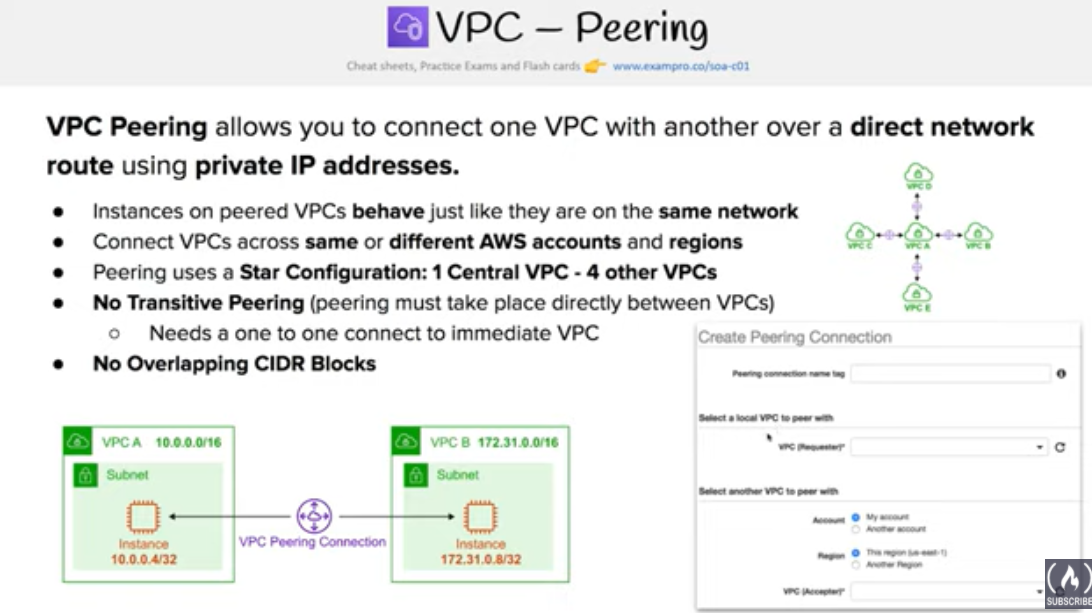
AWS VPC Peering

# VPC Peering Overview

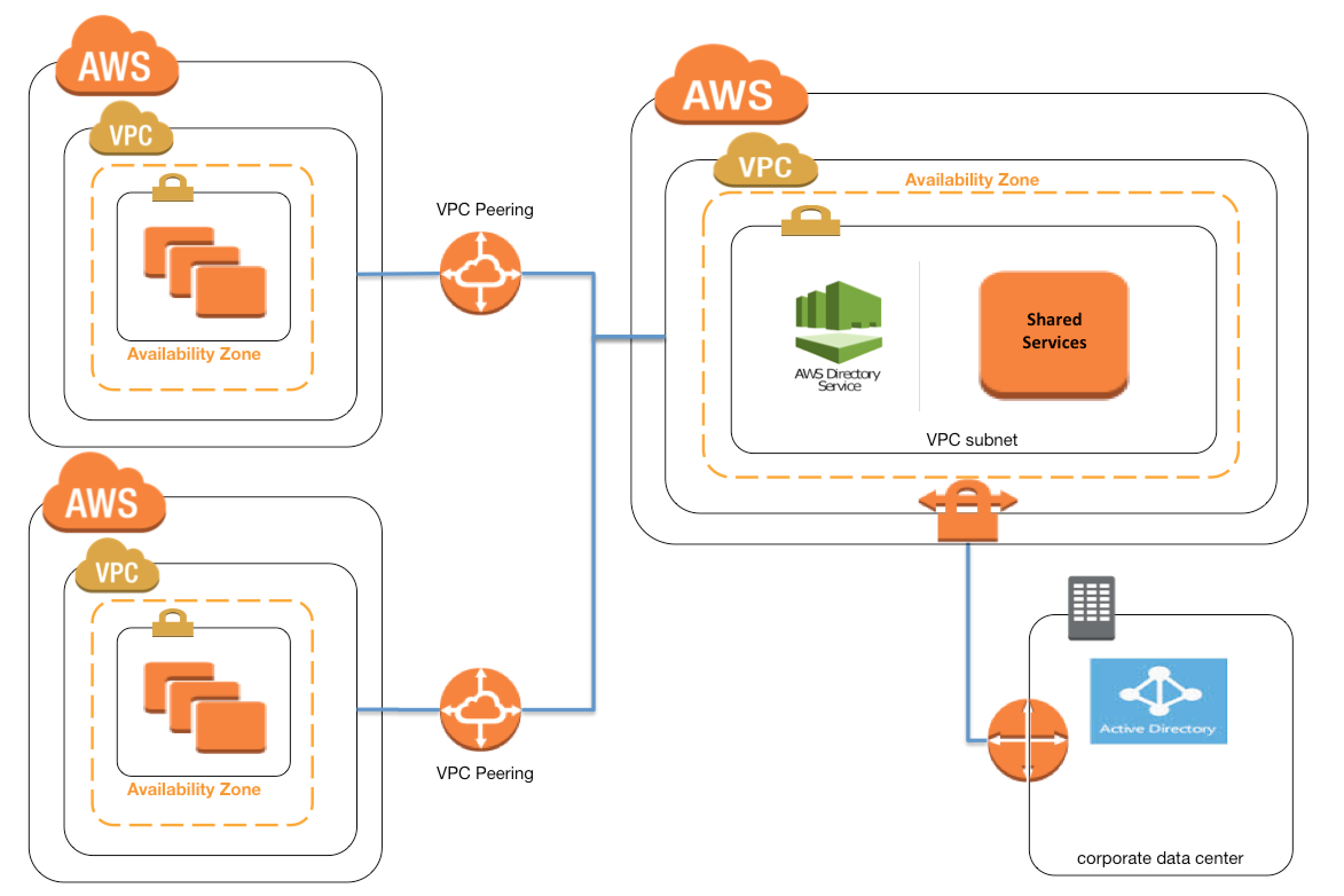
* **A VPC peering connection is a networking connection between two VPCs that enables routing of traffic between them using private IP addresses.**
* Instances in either VPC can communicate with each other as if they are within the same network
* **VPC peering connection can be established between your own VPCs, or with a VPC in another AWS account in a  different region.**
* **AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware.**
* **There is no single point of failure for communication or a bandwidth bottleneck**



## VPC Peering Rules & Limitations

1. **VPC peering connection cannot be created between VPCs that have matching or overlapping CIDR blocks.**
2. (**NOTE** – [VPC Peering is now supported inter-region.](https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/))
3. VPC peering connection are limited on the number active and pending VPC peering connections that you can have per VPC.
4. **VPC peering does not support transitive peering relationships. In a VPC peering connection, the VPC does not have access to any other VPCs that the peer VPC may be peered with even if established entirely within your own AWS account**
5. VPC peering does not support Edge to Edge Routing Through a Gateway or Private Connection
6. **In a VPC peering connection, the VPC does not have access to any other connection that the peer VPC may have and vice versa. Connections that the peer VPC can include**
   1. **A VPN connection or an AWS Direct Connect connection to a corporate network**
   2. **An Internet connection through an Internet gateway**
   3. **An Internet connection in a private subnet through a NAT device**
   4. **A ClassicLink connection to an EC2-Classic instance**
   5. **A VPC endpoint to an AWS service; for example, an endpoint to S3.**
7. Only one VPC peering connection can be established between the same two VPCs at the same time
8. Maximum Transmission Unit (MTU) across a VPC peering connection is 1500 bytes.
9. A placement group can span peered VPCs that are in the**same region**; however, you do not get full-bisection bandwidth between instances in peered VPCs
10. Any tags created for the VPC peering connection are only applied in the account or region in which they were created
11. Unicast reverse path forwarding in VPC peering connections is not supported
12. ~~Instance’s public DNS hostname does not resolve to its private IP address across peered VPCs.~~
13. [Circa July 2016](https://aws.amazon.com/about-aws/whats-new/2016/07/announcing-dns-resolution-support-for-vpc-peering), Instance’s Public DNS can now be resolved to its private IP address across peered VPCs

## VPC Peering Architecture



* VPC Peering can be applied to create shared services or perform authentication with an on-premises instance
* This would help creating a single point of contact, as well limiting the VPN connections to a single account or VPC

**Use case 1 => VPC routing via VPC peering in conflicting Subnet CIDR scenario.**

Graphical user interface, diagram

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**Use case 2 => VPC routing with conflicting IP on-prem data center**

A picture containing graphical user interface

Description automatically generated

**Use case 3 => VPC routing via gateway route table to intercept outgoing & incoming traffic.**

Graphical user interface

Description automatically generated

## AWS Certification Exam Practice Questions

1. A company has an AWS account that contains three VPCs (Dev, Test, and Prod) in the same region. Test is peered to both Prod and Dev. All VPCs have non-overlapping CIDR blocks. The company wants to push minor code releases from Dev to Prod to speed up time to market. Which of the following options helps the company accomplish this?
   1. **Create a new peering connection Between Prod and Dev along with appropriate routes.**
   2. Create a new entry to Prod in the Dev route table using the peering connection as the target.
   3. Attach a second gateway to Dev. Add a new entry in the Prod route table identifying the gateway as the target.
   4. The VPCs have non-overlapping CIDR blocks in the same account. The route tables contain local routes for all VPCs.