**Lecture Notes for AWS Solution Architect**

**MODULE-2**

**VPC Peering**

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor an AWS Site-to-Site 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.



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.

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

You can establish peering relationships between VPCs across different AWS Regions (also called Inter-Region VPC Peering). This allows VPC resources including EC2 instances, Amazon RDS databases and Lambda functions that run in different AWS Regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections, or separate network appliances. The traffic remains in the private IP space. All inter-region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC Peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

**Transit Gateway**

A transit gateway is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks.

**Transit gateway concepts**

The following are the key concepts for transit gateways:

Attachments — You can attach the following:

One or more VPCs

* A Connect SD-WAN/third-party network appliance
* An AWS Direct Connect gateway
* A peering connection with another transit gateway
* A VPN connection to a transit gateway
* **Transit gateway Maximum Transmission Unit (MTU)** — The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The larger the MTU of a connection, the more data that can be passed in a single packet. A transit gateway supports an MTU of 8500 bytes for traffic between VPCs, AWS Direct Connect, Transit Gateway Connect, and peering attachments. Traffic over VPN connections can have an MTU of 1500 bytes.
* **Transit gateway route table** — A transit gateway has a default route table and can optionally have additional route tables. A route table includes dynamic and static routes that decide the next hop based on the destination IP address of the packet. The target of these routes could be any transit gateway attachment. By default, transit gateway attachments are associated with the default transit gateway route table.
* **Associations** — Each attachment is associated with exactly one route table. Each route table can be associated with zero to many attachments.
* **Route propagation** — A VPC, VPN connection, or Direct Connect gateway can dynamically propagate routes to a transit gateway route table. With a Connect attachment, the routes are propagated to a transit gateway route table by default. With a VPC, you must create static routes to send traffic to the transit gateway. With a VPN connection or a Direct Connect gateway, routes are propagated from the transit gateway to your on-premises router using Border Gateway Protocol (BGP). With a peering attachment, you must create a static route in the transit gateway route table to point to the peering attachment.

**Virtual Private Networks**

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.



**AWS Direct Connect**

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space, while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet your changing needs.



**Direct Connect Routing and Link Aggregation Groups (LAGs)**

A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple dedicated connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection. LAGs streamline configuration because the LAG configuration applies to all connections in the group.

In the following diagram, you have four dedicated connections, with two connections to each location. You can create a LAG for the connections that terminate in the same location, and then use the two LAGs instead of the four connections for configuration and management.



You can create a LAG from existing dedicated connections, or you can provision new dedicated connections. After you create the LAG, you can associate existing dedicated connections (whether standalone or part of another LAG) with the LAG.

The following rules apply:

* All connections must be dedicated connections and have a port speed of 1 Gbps, 10 Gbps, or 100 Gbps.
* All connections in the LAG must use the same bandwidth.
* You can have a maximum of two 100G connections, or four connections with a port speed less than 100G in a LAG. Each connection in the LAG counts towards your overall connection limit for the Region.
* All connections in the LAG must terminate at the same AWS Direct Connect endpoint.

**AWS VPC**

Amazon Virtual Private Cloud (Amazon VPC) is a service that lets you launch AWS resources in a logically isolated virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 for most resources in your virtual private cloud, helping to ensure secure and easy access to resources and applications.

As one of AWS's foundational services, Amazon VPC makes it easy to customize your VPC's network configuration. You can create a public-facing subnet for your web servers that have access to the internet. It also lets you place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. Amazon VPC lets you to use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

**Benefits of Using Amazon Virtual Private Cloud (Amazon VPC)**

**Secure and monitored network connections**

Amazon VPC provides advanced security features that allow you to perform inbound and outbound filtering at the instance and subnet level. Additionally, you can store data in Amazon S3 and restrict access so that it’s only accessible from instances inside your VPC. Amazon VPC also has monitoring features that let you perform functions like out-of-band monitoring and inline traffic inspection, which help you screen and secure traffic.

**Simple set-up and use**

With Amazon VPC's simple set-up, you spend less time setting up, managing, and validating, so you can concentrate on building the applications that run in your VPCs. You can create a VPC easily using the AWS Management Console or Command Line Interface (CLI). Once you select from common network setups and find the best match for your needs, VPC automatically creates the subnets, IP ranges, route tables, and security groups you need. After configuring your network, you can easily validate it with Reachability Analyzer.

**Customizable virtual network**

Amazon VPC helps you control your virtual networking environment by letting you choose your own IP Address range, create your own subnets, and configure route tables to any available gateways. You can customize the network configuration by creating a public-facing subnet for your web servers that has access to the internet. Place your backend systems, such as databases or application servers, in a private-facing subnet. With Amazon VPC, you can ensure that your virtual private cloud is configured to fit your specific business needs.

**Use cases**

**Host a simple, public-facing website**

Host a basic web application, such as a blog or simple website, in a VPC and gain the additional layers of privacy and security afforded by Amazon VPC. You can help secure the website by creating security group rules which allow the web server to respond to inbound HTTP and SSL requests from the internet while simultaneously prohibiting the web server from initiating outbound connections to the internet. Create a VPC that supports this use case by selecting "VPC with a Single Public Subnet Only" from the Amazon VPC console wizard.

**Host multi-tier web applications**

Host multi-tier web applications and strictly enforce access and security restrictions between your web servers, application servers, and databases. Launch web servers in a publicly accessible subnet while running your application servers and databases in private subnets. This will ensure that application servers and databases cannot be directly accessed from the internet. You control access between the servers and subnets using inbound and outbound packet filtering provided by network access control lists and security groups. To create a VPC that supports this use case, you can select "VPC with Public and Private Subnets" in the Amazon VPC console wizard.

**Back up and recover your data after a disaster**

By using Amazon VPC for disaster recovery, you receive all the benefits of a disaster recovery site at a fraction of the cost. You can periodically back up critical data from your data center to a small number of Amazon EC2 instances with Amazon Elastic Block Store (EBS) volumes, or import your virtual machine images to Amazon EC2. To ensure business continuity, Amazon VPC allows you to quickly launch replacement compute capacity in AWS. When the disaster is over, you can send your mission critical data back to your data center and terminate the Amazon EC2 instances that you no longer need.

**Extend your corporate network into the cloud**

Move corporate applications to the cloud, launch additional web servers, or add more compute capacity to your network by connecting your VPC to your corporate network. Because your VPC can be hosted behind your corporate firewall, you can seamlessly move your IT resources into the cloud without changing how your users access these applications. Furthermore, you can host your VPC subnets in AWS Outposts, a service that brings native AWS services, infrastructure, and operating models to virtually any data center, co-location space, or on-premises facility. Select "VPC with a Private Subnet Only and Hardware VPN Access" from the Amazon VPC console wizard to create a VPC that supports this use case.

**Securely connect cloud applications to your datacenter**

An IPsec VPN connection between your Amazon VPC and your corporate network encrypts all communication between the application servers in the cloud and databases in your data center. Web servers and application servers in your VPC can leverage Amazon EC2 elasticity and Auto Scaling features to grow and shrink as needed. Create a VPC to support this use case by selecting "VPC with Public and Private Subnets and Hardware VPN Access" in the Amazon VPC console wizard.



**VPC Endpoints**

A VPC endpoint enables private connections between your VPC and supported AWS services and VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink is a technology that enables you to privately access services by using private IP addresses. Traffic between your VPC and the other service does not leave the Amazon network. A VPC endpoint does not require an internet gateway, virtual private gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service.

VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components. They allow communication between instances in your VPC and services without imposing availability risks.

The following are the different types of VPC endpoints. You create the type of VPC endpoint that's required by the supported service.

**Interface endpoints**

An interface endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service. Interface endpoints are powered by AWS PrivateLink.

**Gateway Load Balancer endpoints**

A Gateway Load Balancer endpoint is an elastic network interface with a private IP address from the IP address range of your subnet. Gateway Load Balancer endpoints are powered by AWS PrivateLink. This type of endpoint serves as an entry point to intercept traffic and route it to a service that you've configured using Gateway Load Balancers, for example, for security inspection. You specify a Gateway Load Balancer endpoint as a target for a route in a route table. Gateway Load Balancer endpoints are supported for endpoint services that are configured for Gateway Load Balancers only.

**Gateway endpoints**

A gateway endpoint is for the following supported AWS services:

* Amazon S3
* DynamoDB

**VPC Flow log and DHCP Option Sets**

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After you've created a flow log, you can retrieve and view its data in the chosen destination.

Flow logs can help you with a number of tasks, such as:

* Diagnosing overly restrictive security group rules
* Monitoring the traffic that is reaching your instance
* Determining the direction of the traffic to and from the network interfaces

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency. You can create or delete flow logs without any risk of impact to network performance.

The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network. The options field of a DHCP message contains configuration parameters, including the domain name, domain name server, and the netbios-node-type. When you create a VPC, we automatically create a set of DHCP options and associate them with the VPC. You can configure your own DHCP options set for your VPC.

**Domain-name-servers**

The IP addresses of up to four domain name servers, or AmazonProvidedDNS. If specifying more than one domain name server, separate them with commas. Although you can specify up to four domain name servers, some operating systems may impose lower limits.

To use this option, set it to either AmazonProvidedDNS, or to custom domain name servers. If you set this option to both, the result might cause unexpected behavior.

Default DHCP options set: AmazonProvidedDNS

**Domain-name**

The domain name for your instances. You can specify a custom domain name (for example, example.com). This value is used to complete unqualified DNS hostnames. For more information about DNS hostnames and DNS support in your VPC, see Using DNS with your VPC. If you specify a custom domain name, you must set domain-name-servers to a custom DNS server.

Default DHCP options set: For us-east-1, the value is ec2.internal. For other Regions, the value is region.compute.internal (for example, ap-northeast-1.compute.internal). To use the default values, set domain-name-servers to AmazonProvidedDNS.

**ntp-servers**

The IP addresses of up to four Network Time Protocol (NTP) servers. You can specify the Amazon Time Sync Service at 169.254.169.123. Default DHCP options set: None

**netbios-name-servers**

The IP addresses of up to four NetBIOS name servers.

Default DHCP options set: None

**netbios-node-type**

The NetBIOS node type (1, 2, 4, or 8). We recommend that you specify 2 (point-to-point, or P-node). Broadcast and multicast are not currently supported.

Default DHCP options set: None