**Session 1: Object Storage (S3)**

**1. Compare S3 bucket policies, ACLs, and IAM policies for controlling access. When would you use each?**

* **Bucket Policies:** JSON-based policies applied directly to a bucket. Ideal for granting cross-account access or public access control.
* **ACLs (Access Control Lists):** Legacy method for object-level permissions. Use only for simple, granular access scenarios.
* **IAM Policies:** Attached to users, groups, or roles for identity-based permissions. Best for centralized access control within an account. **When to use:** IAM policies for internal users, bucket policies for external accounts or public access, ACLs for object-level exceptions.

**2. Design a secure S3 bucket setup for a healthcare company to store sensitive patient data.**

* **Encryption:** Enable SSE-KMS for strong encryption and key management.
* **Versioning:** Turn on versioning to protect against accidental deletions.
* **Lifecycle Policies:** Automate archival to Glacier for older data.
* **Logging:** Enable server access logging for audit trails.
* **Block Public Access:** Ensure no public access to comply with HIPAA. This setup ensures confidentiality, integrity, and compliance.

**3. Architecture for static website content delivery with minimal latency worldwide**

* **S3:** Host static content.
* **CloudFront:** Distribute content via global edge locations for low latency.
* **Route 53:** Manage DNS and geo-routing.
* **Security:** Enable HTTPS with ACM, use Origin Access Control (OAC) to restrict direct S3 access, and configure WAF for protection. This architecture ensures performance and security globally.

**Session 2: Networking Components & Routing in VPC**

**4. Compare Internet Gateway, NAT Gateway, Transit Gateway, and VPC Peering**

* **Internet Gateway:** Enables VPC to communicate with the internet.
* **NAT Gateway:** Allows private instances to access the internet without exposing them.
* **Transit Gateway:** Connects multiple VPCs and on-prem networks centrally.
* **VPC Peering:** Direct connection between two VPCs. **Example:** A multi-tier app uses Internet Gateway for public web servers, NAT Gateway for private DB updates, and Transit Gateway for inter-VPC communication.

**5. Inter-region VPC communication strategy**

Use **Transit Gateway with inter-region peering** for low latency and centralized management. This reduces complexity compared to multiple VPC peering links and optimizes cost by avoiding data transfer through public internet.

**6. How VPC routing tables determine traffic flow + misconfiguration scenario**

Routing tables define how traffic exits subnets. Each route specifies a destination CIDR and target (IGW, NAT, TGW).  
**Scenario:** A missing route to NAT Gateway caused private instances to lose internet access.  
**Troubleshooting:**

* Check route table associations.
* Validate target IDs.
* Use VPC Flow Logs to trace dropped packets. Fix by adding correct route for 0.0.0.0/0 to NAT Gateway.