DOMAIN 1: NETWORK DESIGN

- Weight
  - 30% of exam
- Core Skills Covered
  - Designing VPC networks, multi-VPC topologies, and multi-region connectivity
  - Creating hybrid environments (VPN, Direct Connect, Transit Gateway)
  - Selecting appropriate DNS, routing, and traffic distribution strategies
  - Implementing scalable and resilient network designs
- 1.1 Design and Review AWS VPC Architecture
  - Core VPC Components
    - Subnets: Public (has route to IGW), Private (no IGW route)
    - Route Tables: Controls traffic direction within and outside VPC
    - Security Groups: Stateful firewall attached to ENIs
    - NACLs: Stateless rules applied at subnet level
    - Elastic IPs / NAT Gateway: Public IP assignment and outbound Internet from private subnets
    - IGW / EIGW: Internet gateway (IPv4) and egress-only gateway (IPv6)
  - Best Practice
    - Design with multiple AZs, use VPC Peering or Transit Gateway for interconnectivity, and minimize public subnet exposure.
- 1.2 Design Multi-VPC and Multi-Region Architectures
  - VPC Peering vs Transit Gateway (TGW)
    - Type: Point-to-point vs Hub-and-spoke
    - Scaling: Poor at scale (N^2 links) vs Highly scalable
    - Transitive Routing: Not supported vs Supported
    - Route Management: Manual per connection vs Centralized
    - Cost: Data transfer between AZs vs Per-GB pricing + attachments
  - Best Practice
    - Use TGW for multi-VPC/multi-account architectures and centralized egress/NAT.
  - Global Connectivity Options
    - Inter-region traffic: TGW + TGW peering OR VPC peering
    - Global DNS routing: Route 53 + Global Accelerator
    - Private DNS resolution across regions: Route 53 Resolver + forwarding rules
    - Latency-based routing: Route 53 latency policy or Global Accelerator
  - Best Practice
    - TGW peering is non-transitive; for inter-region comms, use VPC peering or TGW peering directly.
- 1.3 Design Hybrid Connectivity to On-Premises
  - VPN and Direct Connect
    - Site-to-Site VPN: IPSec tunnels, supports BGP or static
    - Direct Connect: Dedicated link (1Gbps or 10Gbps), lower latency
    - VPN over DX (Backup): AWS recommends this for HA
    - DX Gateway: Aggregates DX for multiple VPCs
    - Virtual Private Gateway (VGW): Used for VPNs or DX with BGP
    - Customer Gateway (CGW): On-premise end of the tunnel
  - Best Practice
    - Design for redundancy: use multi-AZ VPN tunnels + backup VPN over DX.
  - Key Routing Behaviors
    - VGW automatically advertises AWS routes via BGP
    - Route table must include correct target (VGW, TGW, NAT Gateway, etc.)
    - Longest-prefix match wins in route resolution
    - Route conflicts between TGW and VGW need manual resolution
- 1.4 Design Name Resolution Between Services
  - Amazon Route 53
    - Simple: Single static IP
    - Failover: Active/passive DNS failover
    - Latency-based: Choose lowest latency region
    - Geolocation: Location-specific responses
    - Weighted: Split traffic (e.g. A/B testing)
    - Multivalue answer: Multiple healthy endpoints returned
  - Best Practice
    - CNAMEs not allowed at zone apex, use ALIAS records instead (e.g., for ELB, S3).
  - Route 53 Resolver
    - Inbound endpoints: Allow on-prem → AWS DNS queries
    - Outbound endpoints: Allow AWS → on-prem DNS queries
    - Forwarding rules: Define DNS domain forwarding behavior
    - Query logs: Capture DNS queries via CloudWatch or S3
  - Best Practice
    - Use in hybrid DNS scenarios to allow seamless name resolution.
- 1.5 Design Network Traffic Patterns
  - Load Balancing & Global Traffic
    - ALB (Layer 7): Host/path routing, WebSocket, WAF support
    - NLB (Layer 4): High throughput, TLS termination
    - GWLB: Insert third-party appliances into traffic
    - Global Accelerator: TCP/UDP traffic routing via AWS Edge
    - CloudFront: HTTP caching, CDN for S3 or ALB
  - Best Practice
    - Global Accelerator uses static IPs, accelerates non-HTTP workloads.
- 1.6 Design for High Availability and Fault Tolerance
  - Best Practices
    - VPC: Spread across multiple AZs
    - NAT Gateway: One per AZ (cannot span)
    - VPN: Multiple tunnels per CGW
    - Direct Connect: Redundant connections or DX + VPN fallback
    - Transit Gateway: Attach in multiple AZs
    - Load Balancers: Use ALB/NLB with multi-AZ targets
    - Route 53: Health checks + failover routing policy
  - Best Practice
    - Don't forget CloudWatch alarms and autoscaling for app-level HA.
- Sample ANS-C01 Scenarios (Domain 1)
  - You need to connect 25 VPCs across 5 accounts. What's the best option? ➤ Use AWS Transit Gateway for hub-and-spoke architecture.
  - You want on-prem DNS servers to resolve AWS private records. ➤ Create Route 53 Resolver inbound endpoint in AWS.
  - Your VPN fails and you want to keep a DX active. ➤ Use DX primary, VPN as backup, and BGP for failover.
  - Design a multi-region app with lowest latency routing. ➤ Use Route 53 latency routing or Global Accelerator.
  - Need centralized security appliances (firewalls). ➤ Use Gateway Load Balancer (GWLB) with inline insertion.
- Summary Cheat Sheet
  - Multi-VPC Hub-Spoke: Transit Gateway
  - Multi-Region Low Latency: Global Accelerator
  - Hybrid DNS: Route 53 Resolver
  - Secure Hybrid Connectivity: Direct Connect + Site-to-Site VPN
  - Centralized NAT: NAT Gateway in each AZ
  - Resilient Load Balancing: ALB/NLB + multi-AZ
  - DNS Health Checks: Route 53 failover routing
  - Inter-region VPC comms: VPC Peering or TGW Peering
- Must-Read AWS Resources
  - VPC Best Practices
  - Hybrid Connectivity Whitepaper
  - Transit Gateway Documentation
  - Route 53 Routing Policies
  - Global Accelerator Guide
  - AWS Network Design Patterns

Presented with xmind AI