AWS Certified Advanced Networking - Specialty Cheat Sheet

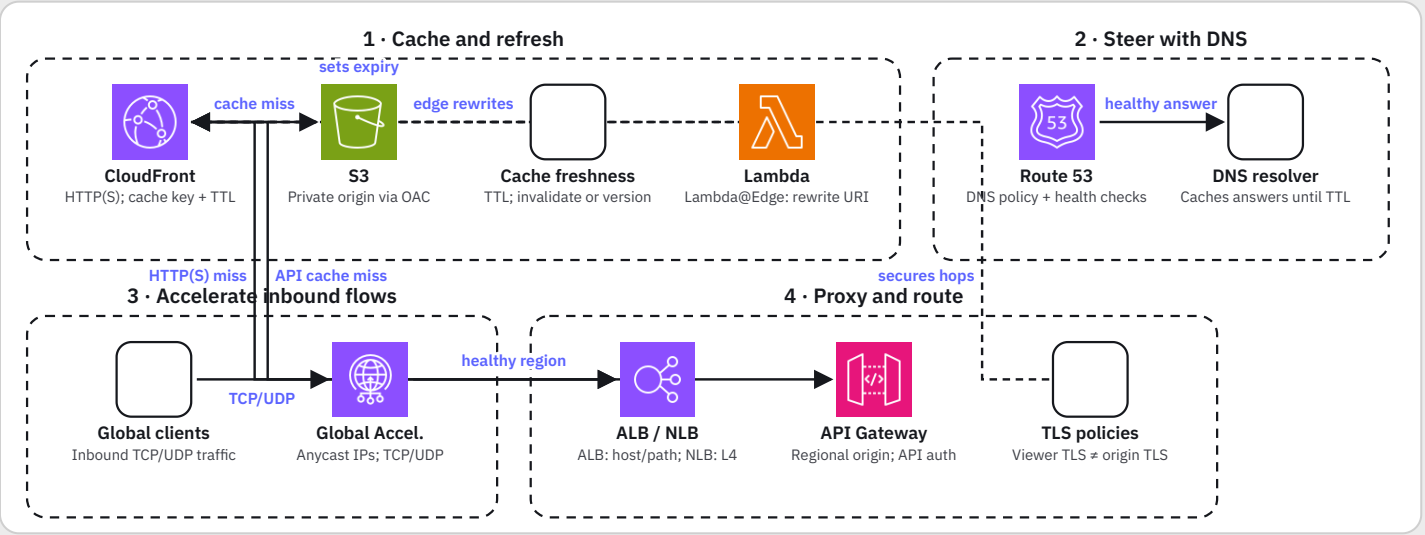
ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · 30% OF THE EXAM · TASK STATEMENT 1.1

Design a solution that incorporates edge network services to optimize user performance and traffic management for global architectures

Cache, steer, accelerate, route



1 Cache and refresh

Choose **cacheable HTTP(S)** to lower latency and origin load; cache keys control reuse, TTL controls freshness. Invalidate or version changed objects. Measure hit ratio, delivery throughput, and data egress cost.

2 Steer with DNS

Choose **DNS routing** for latency-based, weighted, or failover policies. Health checks change future answers; resolver TTLs delay convergence, so failover is not instantaneous.

3 Accelerate inbound flows

Choose **static anycast IPs** for fixed-IP or non-HTTP ingress. Health checks steer new flows to healthy regional endpoints over the AWS global network; traffic is not cached.

4 Proxy and route

Use **Layer 7 routing** for host/path rules on ALB; NLB handles Layer 4. Amazon CloudFront reverse-proxies ALB or regional APIs; configure viewer and origin TLS separately.

Exam traps

- A **cache invalidation** removes edge copies, not browser caches; versioned URLs bypass old objects. TTL expiration does not proactively push fresh content to every edge.
- **AWS Global Accelerator endpoints** include ALB/NLB, not Amazon S3, Amazon CloudFront, or Amazon API Gateway. An API origin behind Amazon CloudFront is not automatically an accelerator endpoint.
- **Outbound internet egress** is not accelerated by placing AWS Global Accelerator in front of an app. Amazon CloudFront optimizes HTTP(S) delivery; delivery traffic is still billed.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

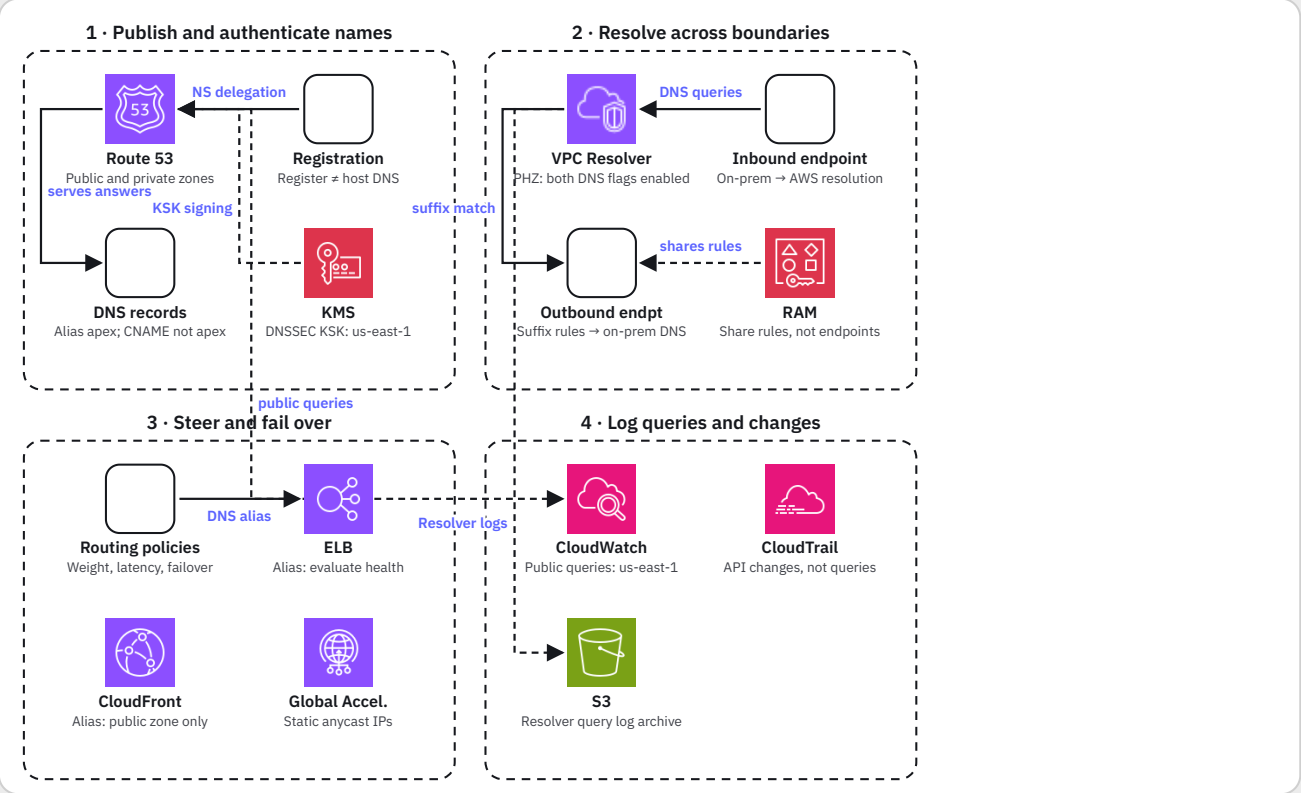
ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · TASK STATEMENT 1.2

Design DNS solutions that meet public, private, and hybrid requirements

Publish, resolve, steer, observe



1 Publish and authenticate names

Registration and hosting are separate. Parent NS records delegate to hosted-zone nameservers. **DNSSEC** requires a parent DS record; it authenticates answers, not encryption. Only public hosted zones support signing.

2 Resolve across boundaries

Use **conditional forwarding** over Direct Connect or VPN; allow UDP/TCP 53. Endpoints are Regional, with IPs in at least two AZs. Associate shared hub rules with spoke VPCs; the most-specific matching rule wins.

3 Steer and fail over

Choose **latency or weighted** for multi-Region active-active; failover for primary/secondary. Private targets can use CloudWatch-alarm health checks. Global Accelerator steers connections, rather than relying on DNS changes.

4 Log queries and changes

Enable **query logging** separately: public hosted zones → CloudWatch Logs; VPC Resolver queries → CloudWatch Logs or S3. Configure log retention or S3 lifecycle explicitly. Resolver cache hits do not generate query logs.

Exam traps

- **Private-zone match** has no public fallback: missing records return NXDOMAIN. The most-specific associated zone wins; a forwarding rule for the same domain overrides the private hosted zone.
- **DNS failover is cached**: TTL delays changed answers reaching clients. Health checks cannot revoke cached answers or directly probe private IPs; ELB aliases can evaluate target health.
- **Cross-account PHZ association** needs zone-owner authorization and VPC-owner association, not RAM. VPC peering alone does not associate private hosted zones.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

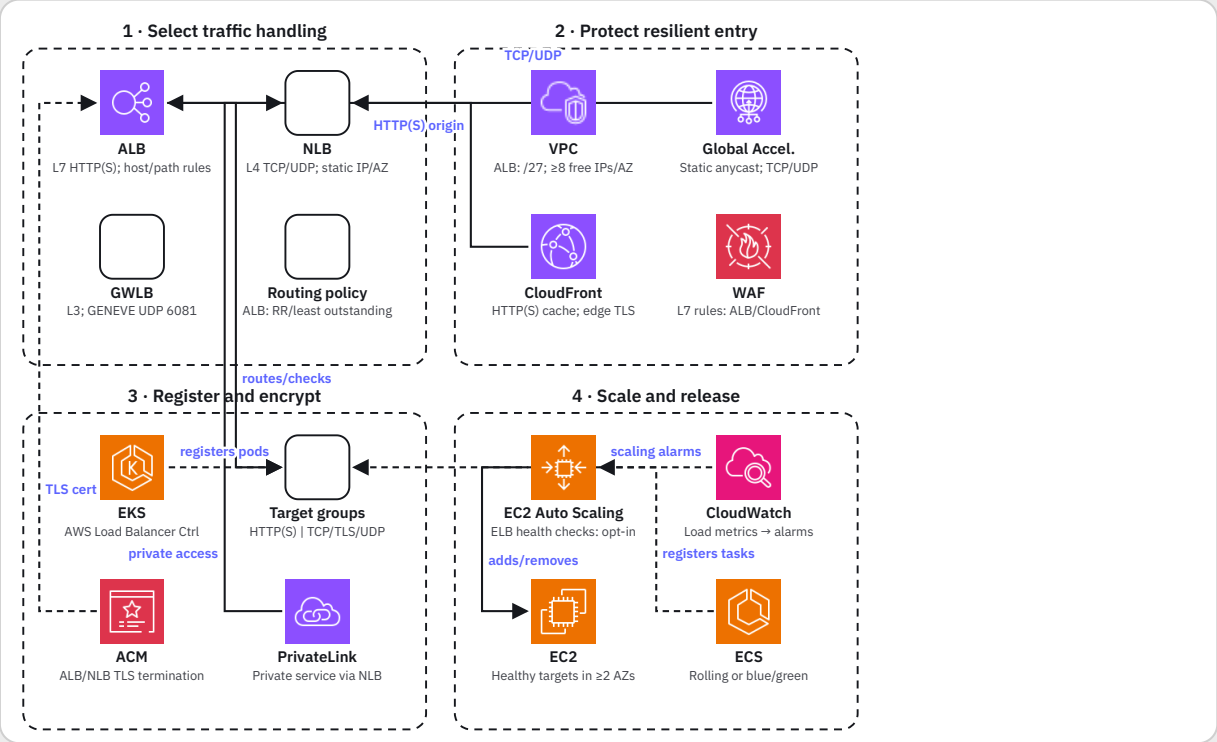
ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · TASK STATEMENT 1.3

Design solutions that integrate load balancing to meet high availability, scalability, and security requirements

Select, protect, register, scale



1 Select traffic handling

Choose **L7** ALB for host/path routing and WAF; NLB for TCP/UDP, static IPs or PrivateLink; GWLB for transparent appliances. NLB distributes flows by hash, not least connections.

2 Protect resilient entry

Multi-AZ targets provide HA. ALB cross-zone is on at LB level; NLB/GWLB default off. Internal LBs use private IPs; internet-facing LBs need public subnets, not public targets.

3 Register and encrypt

Controller needs IAM permissions: Ingress→ALB, LoadBalancer Service→NLB. Instance targets use NodePort; IP targets reach pods. NLB TCP passes TLS through; a TLS listener terminates with ACM.

4 Scale and release

Scale targets with ASG; ELB scales separately, not instantly. Enable ELB health checks for ASG replacement; deregistration delay drains scale-in. ALB weighted target groups shift canary/blue-green traffic.

Exam traps

- **TLS passthrough** needs NLB TCP, not TLS; ALB terminates TLS. ALB supports Cognito/OIDC authentication; NLB does not. HTTPS to targets encrypts again but does not validate their certificates.
- **Client IP**: ALB uses X-Forwarded-For; NLB can preserve source IP or send PROXY v2 to compatible targets. ALB stickiness uses cookies; NLB uses source-IP affinity.
- **Health checks** can fail open when all targets are unhealthy. Stickiness does not replicate sessions; weighted target groups do not automatically fail over to healthy groups.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

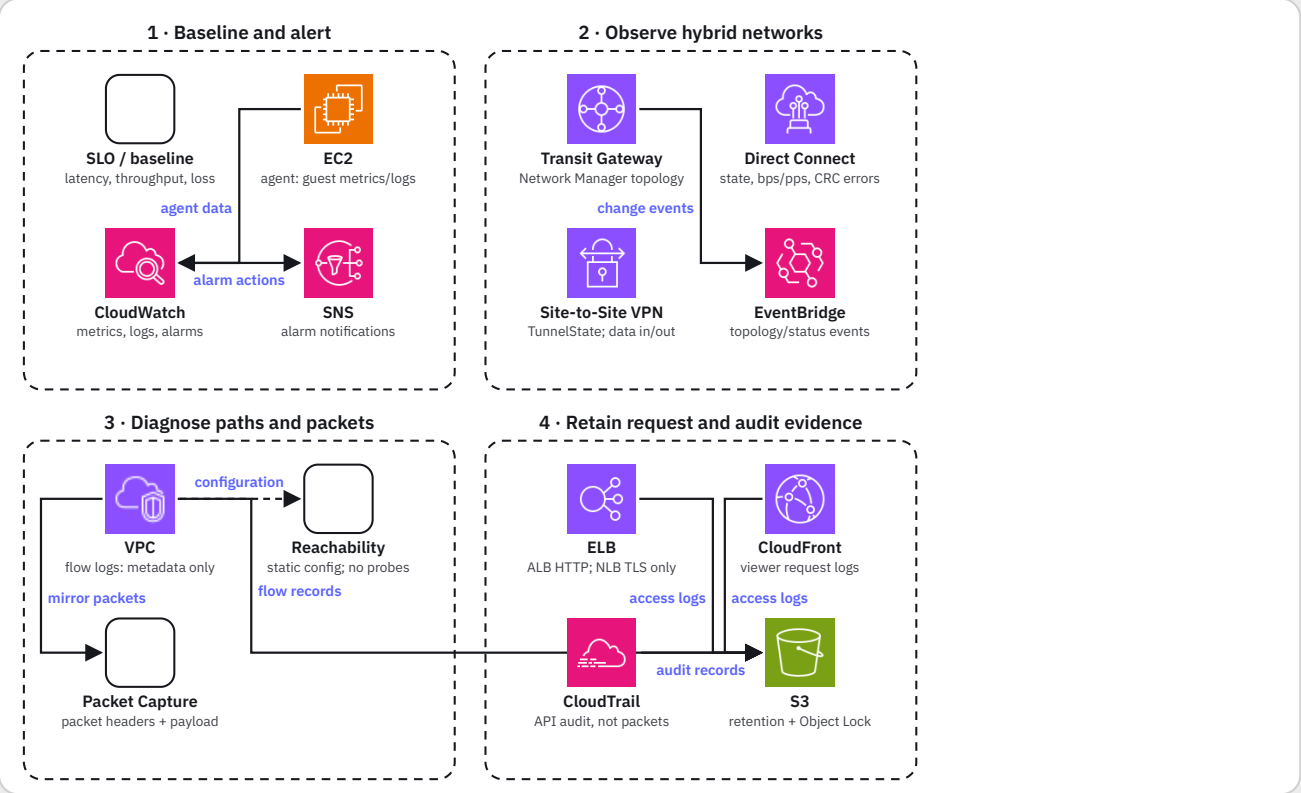
ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · TASK STATEMENT 1.4

Define logging and monitoring requirements across AWS and hybrid networks

Baseline, observe, trace, retain



1 Baseline and alert

SLOs set targets; benchmark and load-test representative traffic before setting alarms. EC2 agents add guest telemetry; dashboards visualize metrics, and Logs Insights queries logs.

2 Observe hybrid networks

Hybrid visibility uses Network Manager for topology/events and CloudWatch for link/tunnel metrics. Measure latency and packet loss with endpoint probes; interface counters alone do not establish either.

3 Diagnose paths and packets

Packets require Traffic Mirroring on supported ENIs to a capture sensor; flow logs send ACCEPT/REJECT metadata to CloudWatch Logs or S3. Reachability Analyzer models supported paths, not live delivery.

4 Retain request and audit evidence

Request logs diagnose edge/load-balancer requests; CloudTrail audits API actions. Enable log delivery to S3 and set lifecycle retention; Object Lock protects immutable audit history.

Exam traps

- **Flow logs are not packet capture**: ACCEPT/REJECT records omit payload and arrive asynchronously; Traffic Mirroring copies supported ENI traffic, not every AWS network hop.
- **Reachability Analyzer is not a ping**: it evaluates supported configuration paths; a reachable result does not prove application health, latency, or absence of packet loss.
- **CloudWatch Logs retention defaults to never expire**; S3 lifecycle is separate. Collecting logs does not automatically establish compliant retention or protect records from deletion.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

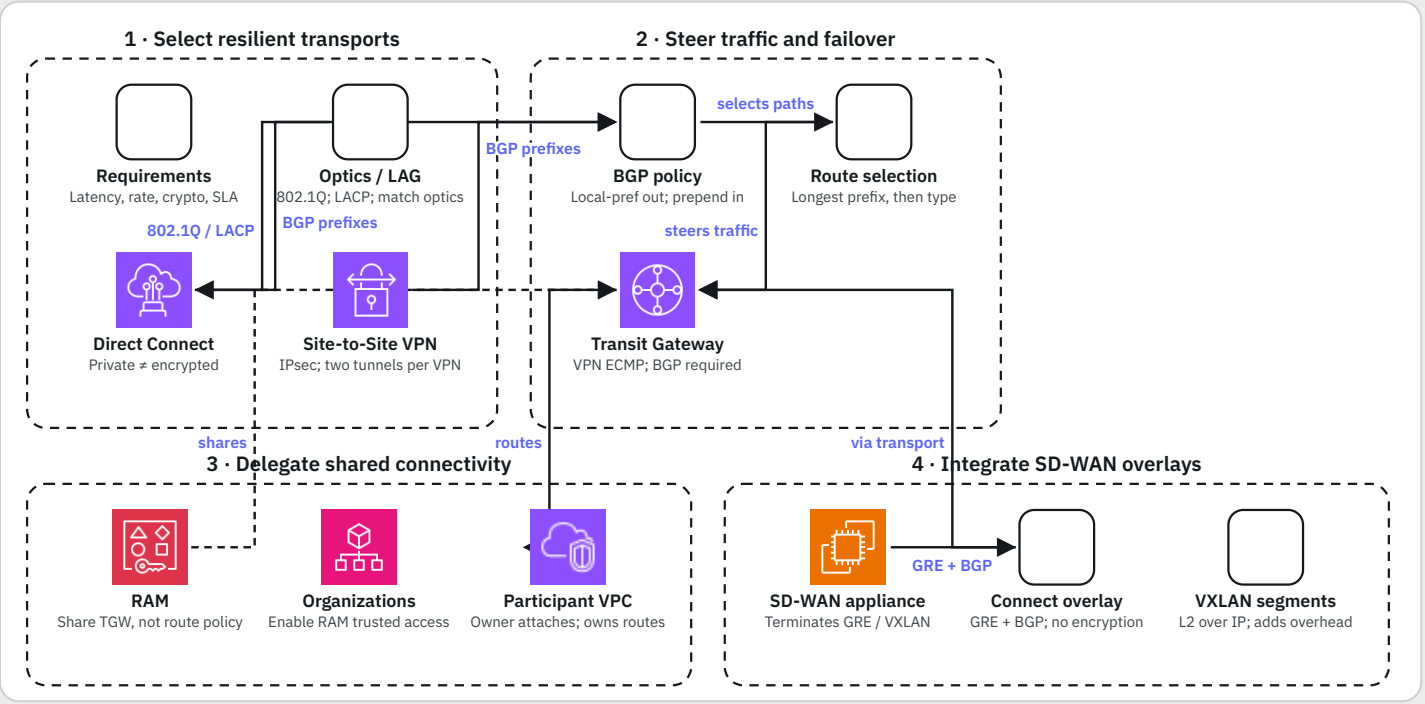
ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · TASK STATEMENT 1.5

Design a routing strategy and connectivity architecture between on-premises networks and the AWS Cloud

Connect, steer, share, encapsulate



1 Select resilient transports

Predictable throughput favors Direct Connect; rapid encrypted connectivity favors VPN. Diversify routers, carriers and DX locations. Jumbo MTU support: DX private/transit 9001/8500; VPN maximum 1446; account for overhead.

2 Steer traffic and failover

Active/active needs equal BGP paths and ECMP; active/passive uses local preference and AS-path prepending. BGP withdrawal enables failover. TGW equal-prefix static routes beat propagated routes; tables segment traffic.

3 Delegate shared connectivity

Cross-account: RAM shares TGW; VPC owners create attachments and VPC routes, while the TGW owner controls associations and propagation. Direct Connect gateway associations use cross-account proposals, not RAM.

4 Integrate SD-WAN overlays

TGW Connect uses GRE+BGP over a VPC or Direct Connect transport attachment; it is not IPsec. VXLAN terminates on appliances, not TGW. Overlay segmentation still requires enforced routing and security controls.

Exam traps

- **LAG ≠ path diversity**: members share a Direct Connect location. Surviving a location failure requires another location and independent paths; one flow is still limited to one member link.
- **Direct Connect is not encrypted by default**. IPsec supplies end-to-end protection; MACsec on supported dedicated connections protects the Ethernet link, not the entire application path.
- **Static VPN routing is unsupported on TGW**; use BGP. ECMP distributes flows across eligible equal paths, not packets into a single faster flow.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

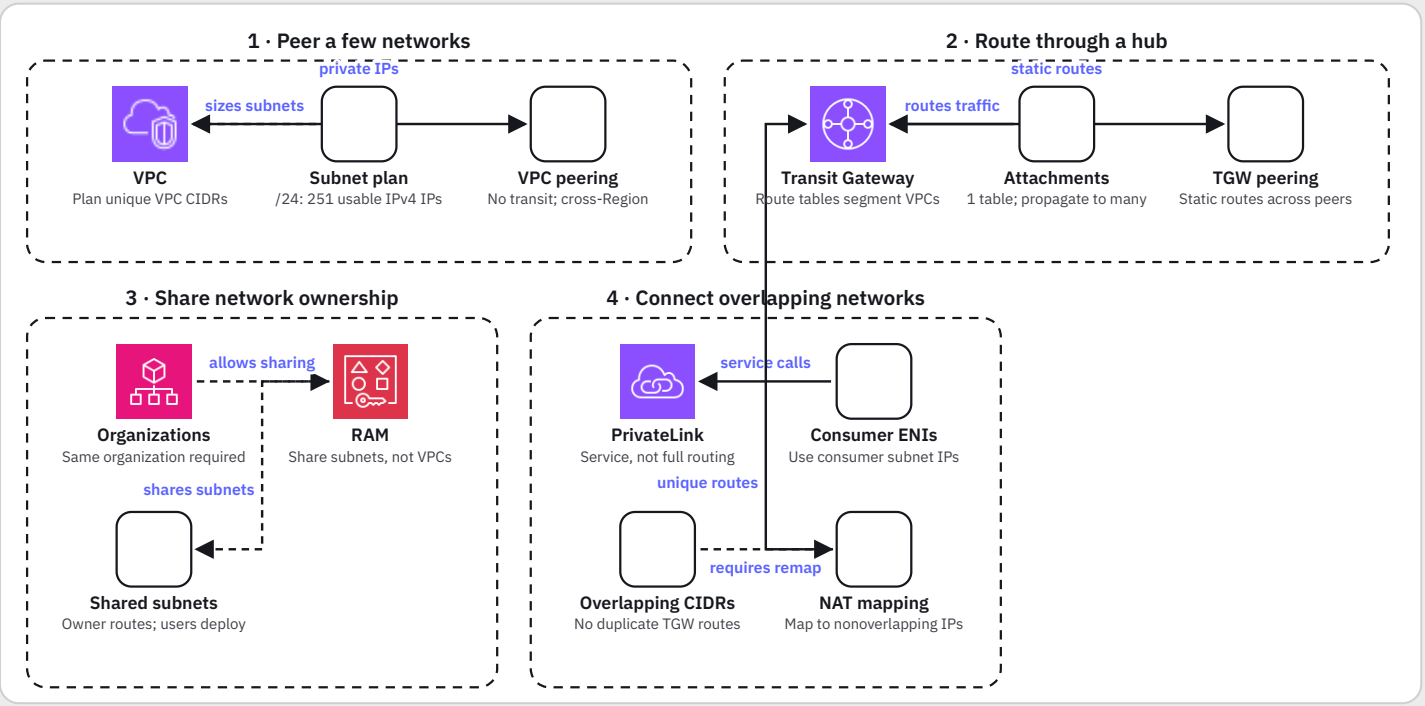
ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · TASK STATEMENT 1.6

Design a routing strategy and connectivity architecture that include multiple AWS accounts, AWS Regions, and VPCs to support different connectivity patterns

Peer, route, share, translate



1 Peer a few networks

Use **VPC peering** for direct connectivity between a few VPCs with nonoverlapping CIDRs, including across accounts or Regions. Configure routes on both sides and permit traffic through security groups and NACLs.

2 Route through a hub

Use **Transit Gateway** for scalable, transitive hub-and-spoke connectivity. Share it across accounts with RAM. Each attachment associates with one route table; selective propagation and routes enforce segmentation.

3 Share network ownership

For **central network ownership**, enable sharing with Organizations in RAM, then share subnets within the organization. The owner manages networking; participants create and own workload resources.

4 Connect overlapping networks

For **overlapping CIDRs**, use PrivateLink for service-only access; otherwise renumber or explicitly translate addresses to unique ranges. TGW alone does not resolve overlap.

Exam traps

- A–B and B–C peering do not connect A–C: peering is **nontransitive**. A peer also cannot use another VPC's internet gateway, NAT gateway, or VPN connection as a transit path.
- TGW attachment propagation does not imply **peering propagation**. TGW peering requires static routes; inter-Region peering does not automatically exchange VPC routes.
- VPC sharing is not **network isolation**: participants own their resources, but subnets use the owner's VPC routing. Account boundaries do not replace security groups and NACLs.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Cheat Sheet

ANS-C01 · Domain 1 of 4

BlowStack

DOMAIN 1 · NETWORK DESIGN · WHAT TO REMEMBER

Concepts and services of Network Design

Concepts to know

IP Routing

Routing selects paths by destination prefix; **longest-prefix match** favors the most specific route. Connectivity requires valid forward and return paths; peering is nontransitive, while transit architectures require explicit routing and segmentation.

High availability

Availability depends on **independent failure domains**, health detection, and usable surviving capacity. Multiple links at one location do not provide location resilience; hybrid designs must preserve routing and capacity after failure.

DNS

DNS maps names to records and supports traffic steering. **Resolver direction and namespace scope** determine hybrid designs: inbound endpoints accept on-premises queries; outbound endpoints forward matching queries toward on-premises DNS.

Core services



Amazon Route 53

Use **private hosted zones** for VPC namespaces and Resolver endpoints for hybrid resolution. Public routing policies support weighted, latency, and failover decisions; cached answers delay changes.



Elastic Load Balancing (ELB)

Choose **ALB for HTTP-aware routing**, NLB for TCP/UDP or static IP requirements, and GWLB for transparent appliance insertion with GENEVE. TLS passthrough requires a TCP listener rather than termination.



AWS Transit Gateway

Use **route tables for segmentation** in transitive VPC and hybrid networks. Associations select ingress lookup tables; propagation installs routes. Overlapping CIDRs require translation or isolation.

Get practice exams and lessons for AWS Certified Advanced Networking - Specialty