AWS Certified Advanced Networking - Specialty Cheat Sheet

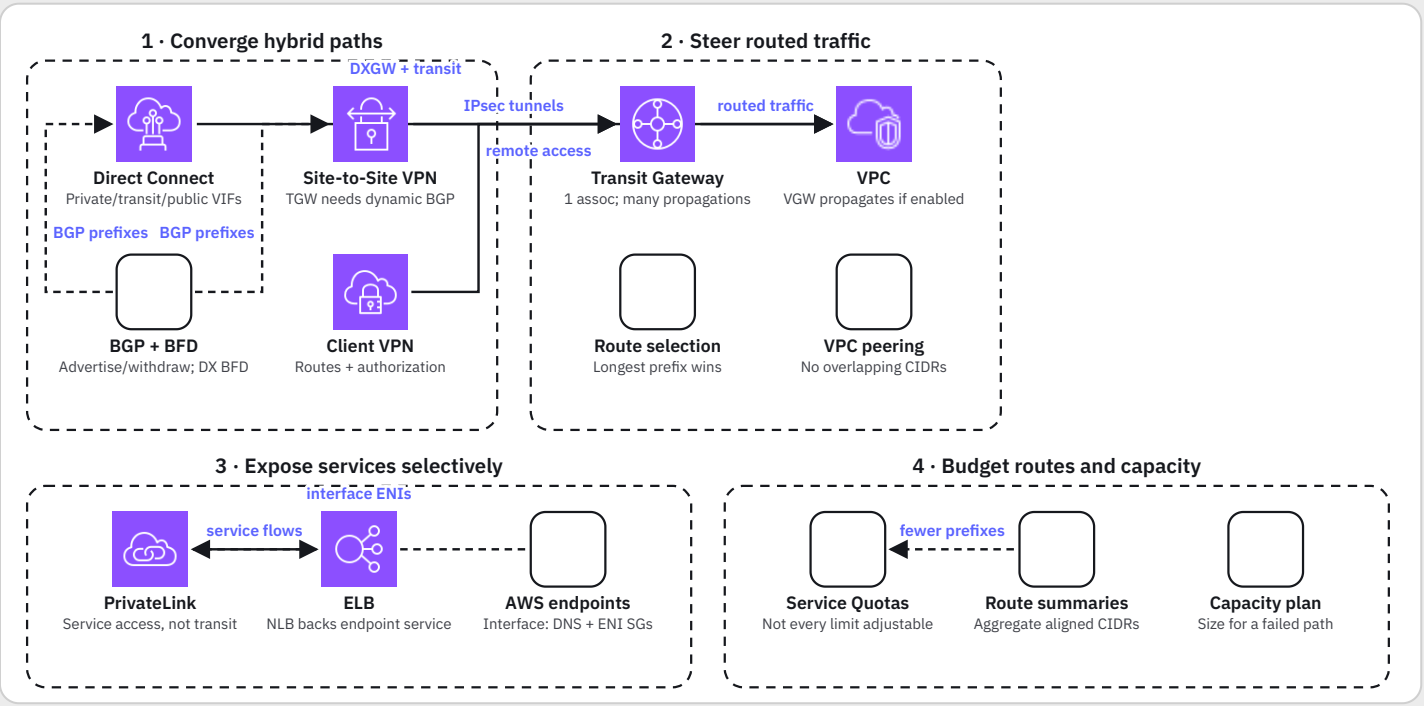
ANS-C01 · Domain 3 of 4

BlowStack

DOMAIN 3 · NETWORK MANAGEMENT AND OPERATION · 20% OF THE EXAM · TASK STATEMENT 3.1

Maintain routing and connectivity on AWS and hybrid networks

Converge, steer, expose, rightsize



1 Converge hybrid paths

Use **transit VIF** + Direct Connect gateway for TGW; private VIF for VGW, public VIF for AWS public endpoints. VPN encrypts; DX alone does not. BFD is supported on DX, not AWS VPN.

2 Steer routed traffic

Use **hub-and-spoke** for transit; VPC peering is nontransitive within or across Regions. TGW peering uses static routes; propagation does not cross the peering attachment.

3 Expose services selectively

Use **PrivateLink** + NLB for private custom services, including overlapping CIDRs; internet-facing ELB for public apps. Interface endpoints use private IPs; S3/DynamoDB gateway endpoints install routes.

4 Budget routes and capacity

Route budgets apply to VPC/TGW tables and DX/VPN advertisements; excess BGP routes can drop a session. Check adjustable quotas and bandwidth limits; summarize without hiding unreachable subnets.

Exam traps

- **Association is not propagation**: a TGW attachment's association selects its ingress lookup table; propagation adds routes. VPC peering cannot provide onward transit to VPN, DX, or another peer.
- **Longest prefix wins** before route type; at an equal prefix, static beats propagated in VPC/TGW tables. Independent return routes can break stateful inspection through asymmetry.
- **ECMP is per flow**, not link bonding: TGW can spread BGP VPN flows, not one flow across tunnels. Summaries reduce route count but can blackhole traffic if component routes fail.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

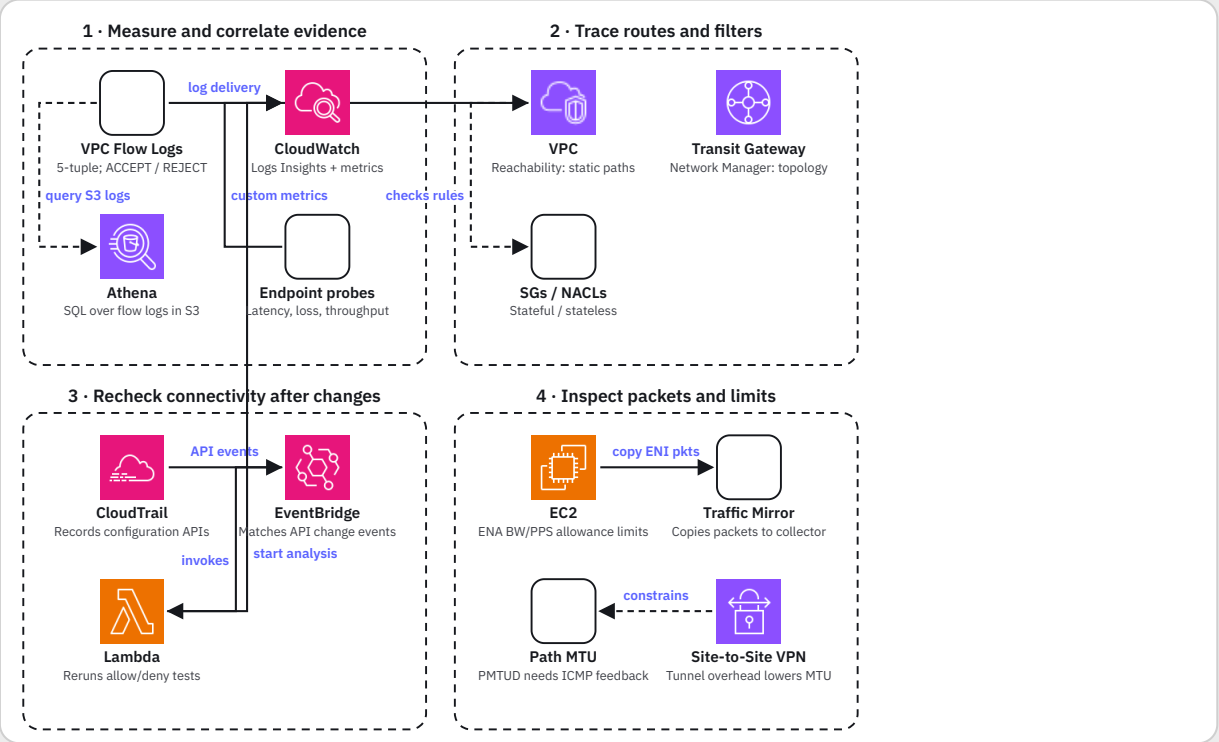
ANS-C01 · Domain 3 of 4

BlowStack

DOMAIN 3 · NETWORK MANAGEMENT AND OPERATION · TASK STATEMENT 3.2

Monitor and analyze network traffic to troubleshoot and optimize connectivity patterns

Measure, trace, verify, inspect



1 Measure and correlate evidence

Packet loss needs probes or endpoint counters; Flow Logs summarize traffic, not payloads. Correlate timestamps with latency and throughput; use Logs Insights for CloudWatch logs, Athena for logs in S3.

2 Trace routes and filters

Reachability Analyzer models routes and filters, not live performance. Check longest-prefix routes and both directions; NACLs need return ephemeral ports. TGW route tables control hub-and-spoke segmentation.

3 Recheck connectivity after changes

Configuration drift triggers regression checks through CloudTrail, EventBridge and Lambda. Compare analyzed paths with approved allow/deny intent; this workflow must be built, not enabled automatically by Reachability Analyzer.

4 Inspect packets and limits

Large transfers stall: check path MTU and ICMP; lower MTU or clamp TCP MSS. Packet captures expose retransmissions and TCP window changes; token-bucket shaping permits bursts but limits sustained throughput.

Exam traps

- **ACCEPT does not prove delivery**: Flow Logs show permitted traffic at the capture point, not end-to-end success. REJECT indicates filtering, not a measured packet-loss percentage.
- **Reachable is not fast**: Reachability Analyzer sends no packets and measures no latency or throughput. A topology map alone proves neither route propagation nor segmentation.
- **Jumbo MTU is not end-to-end**: the smallest path MTU wins. Site-to-Site VPN does not support PMTUD; configure suitable MTU/MSS. MSS clamping fixes TCP segment size, not UDP datagrams.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

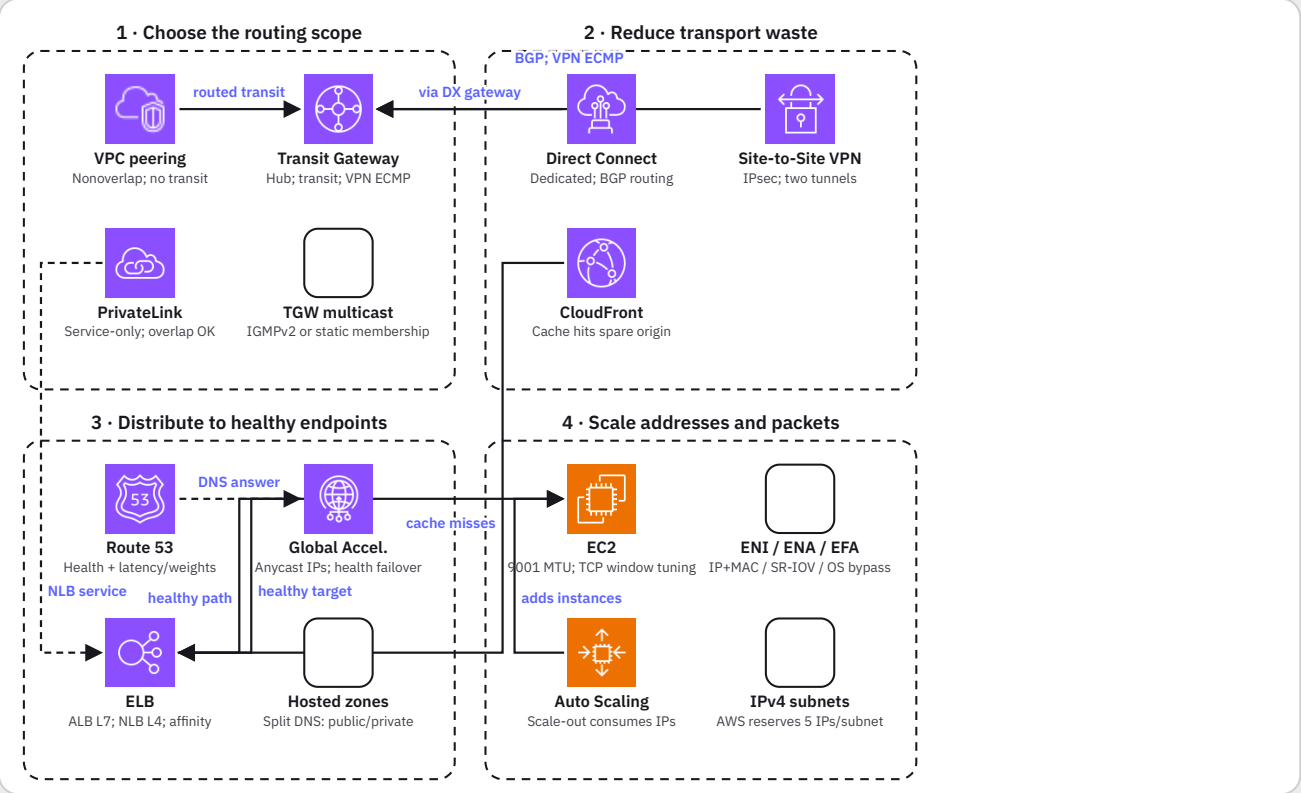
ANS-C01 · Domain 3 of 4

BlowStack

DOMAIN 3 · NETWORK MANAGEMENT AND OPERATION · TASK STATEMENT 3.3

Optimize AWS networks for performance, reliability, and cost-effectiveness

Connect, cache, distribute, scale



1 Choose the routing scope

Peering fits a few nonoverlapping VPCs without transit; TGW scales routed hubs. PrivateLink exposes a service, not whole networks. Longest prefix wins; configure forward and return routes.

2 Reduce transport waste

Steady high volume can favor Direct Connect after port, provider and egress costs; VPN suits quick, low-volume access. DX is not encrypted by default. Resilience requires redundant paths; one DX connection is insufficient.

3 Distribute to healthy endpoints

Global Accelerator improves TCP/UDP paths without caching; CloudFront caches HTTP(S). Route 53 selects DNS answers using health and routing policy; TTL delays changes. ALB routes by host/path; affinity can skew load.

4 Scale addresses and packets

Subnets cannot resize: add secondary VPC CIDRs and new subnets; update scaling placement across AZs. Reserve IP headroom for instances and ELB. TCP window scaling helps high bandwidth-delay paths; EFA needs compatible software.

Exam traps

- **Private DNS is not public fallback**: a matching private hosted zone with no matching record returns NXDOMAIN. Private targets need supported alias health evaluation or custom health signals.
- TGW **multicast is VPC-only**, not native across DX, VPN or peering; tunnel it to on-premises. VPN ECMP increases aggregate throughput across flows, not the speed of one flow.
- **MTU is path-limited**: EC2 9001; TGW 8500; DX private VIF 9001, transit VIF 8500; internet 1500; VPN ≤1446. Allow PMTUD ICMP where supported; fragmentation adds overhead.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

ANS-C01 · Domain 3 of 4

BlowStack

DOMAIN 3 · NETWORK MANAGEMENT AND OPERATION · WHAT TO REMEMBER

Concepts and services of Network Management and Operation

Concepts to know

Longest Prefix Match

The most specific matching destination prefix wins before equal-prefix route priorities apply. Choose routes by **prefix specificity**, then check service-specific precedence and the return path.

Border Gateway Protocol

BGP exchanges hybrid network prefixes and selects paths. Use **route advertisements and path attributes** to control preference; ECMP requires eligible equal-cost paths, and BFD accelerates failure detection on supported Direct Connect sessions.

Maximum Transmission Unit

MTU limits packet size on each link; the smallest path MTU constrains end-to-end traffic. When small packets work but transfers stall, check **path MTU and tunnel overhead**; jumbo frames require path-wide support.

Core services



AWS Transit Gateway

Choose **transitive hub-and-spoke routing** for many VPCs and hybrid networks. Attachment association selects the lookup table; propagation installs learned routes into selected tables.



Amazon VPC

Choose peering for direct, nontransitive connectivity. Use **Reachability Analyzer for configuration paths**, Flow Logs for traffic metadata, and Traffic Mirroring for packet inspection.



AWS Direct Connect

Choose dedicated hybrid connectivity for predictable performance. Select **private, transit, or public VIFs** for virtual private gateway access, transit gateway access, or public AWS endpoints.

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