AWS Certified Advanced Networking - Specialty Cheat Sheet

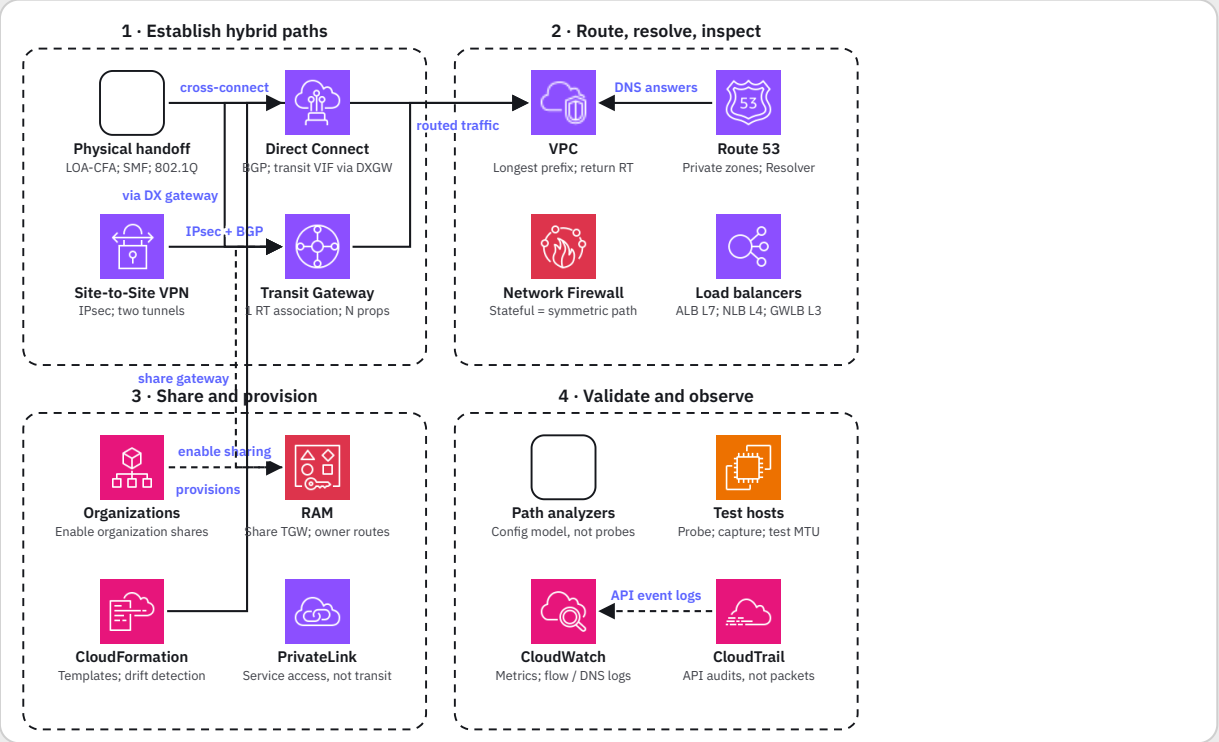
ANS-C01 · Domain 2 of 4

BlowStack

DOMAIN 2 · NETWORK IMPLEMENTATION · 26% OF THE EXAM · TASK STATEMENT 2.1

Implement routing and connectivity between on-premises networks and the AWS Cloud

Connect, route, share, validate



1 Establish hybrid paths

Transit VIF connects DX to TGW through a DX gateway. TGW VPN requires BGP; ECMP uses equal paths. TGW Connect uses GRE+BGP, not encryption. Separate TGW route tables enforce routing segmentation.

2 Route, resolve, inspect

Inbound Resolver receives on-premises queries; outbound endpoints + rules forward AWS queries on premises. Stateful inspection needs symmetric paths; TGW appliance mode preserves AZ affinity.

3 Share and provision

AWS RAM shares TGWs, subnets and Resolver rules. Sharing does not install routes: the TGW owner manages gateway tables; participants manage VPC routes. CloudFormation drift detection does not repair drift.

4 Validate and observe

Reachability Analyzer models VPC configuration; Route Analyzer checks TGW routes, not live packets. Probe both directions; allow ICMP for PMTUD. Flow/query logs need enabling and retention settings.

Exam traps

- **Dedicated ≠ encrypted**: DX does not encrypt by default; use IPsec or supported MACsec. A LAG at one DX location is not multi-location resilience.
- **Longest prefix first**: route-source preference breaks equal-prefix ties. For equal TGW prefixes, static beats propagated; a less-specific static route does not beat a more-specific BGP route.
- **PrivateLink is not peering**: it exposes a service, not arbitrary network transit. Overlapping CIDRs need translation or service-level access; adding TGW routes does not remove the overlap.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

ANS-C01 · Domain 2 of 4

BlowStack

DOMAIN 2 · NETWORK IMPLEMENTATION · TASK STATEMENT 2.2

Implement routing and connectivity across multiple AWS accounts, Regions, and VPCs to support different connectivity patterns

Route, share, resolve, inspect



1 Route across networks

Use **Transit Gateway** for transitive hub-and-spoke routing. Each attachment associates with one table and can propagate to many. Configure VPC return routes; inter-Region TGW peering needs static routes.

2 Deploy and share services

Use **PrivateLink** for consumer-initiated service access, including overlapping CIDRs, not network transit. RAM shares a TGW, not routing ownership; StackSets deploy repeatably, while drift detection identifies supported changes.

3 Resolve and authorize clients

Resolver **inbound** endpoints receive on-premises queries; outbound endpoints plus conditional rules reach corporate DNS. Client VPN needs authentication, authorization rules, and routes; IAM permissions do not permit packets.

4 Inspect and verify flows

Stateful inspection needs **symmetric routing**; TGW appliance mode preserves flow AZ affinity. Flow logs contain metadata, not payload. Reachability Analyzer models configuration; live probes test delivery.

Exam traps

- VPC peering is **non-transitive** and rejects overlapping CIDRs; a peer cannot provide transit to its VPN or Direct Connect connection.
- Direct Connect is **not encrypted by default**. A private circuit does not imply IPsec; use Site-to-Site VPN over Direct Connect when end-to-end IPsec encryption is required.
- A matching **private hosted zone** without a matching record returns NXDOMAIN, not public DNS fallback. Cross-account zone association is separate from RAM Resolver-rule sharing.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

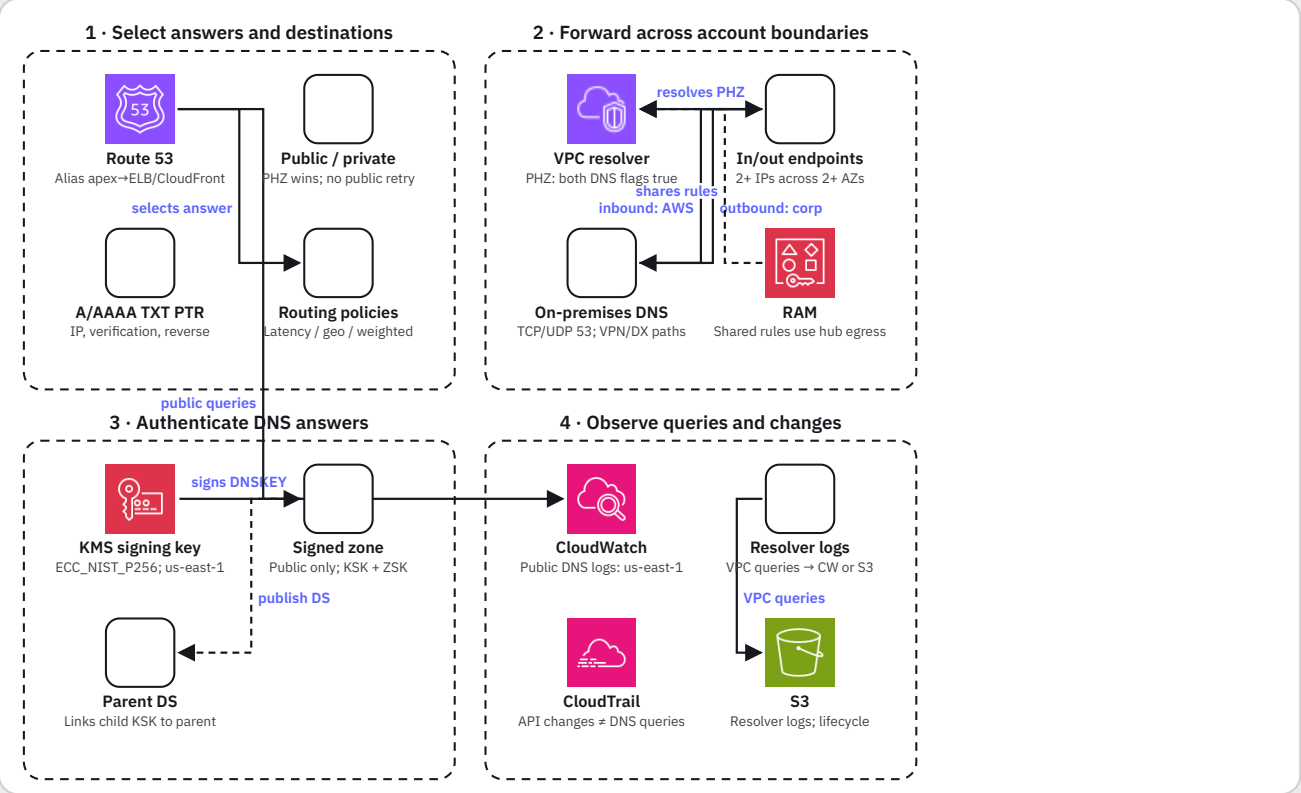
ANS-C01 · Domain 2 of 4

BlowStack

DOMAIN 2 · NETWORK IMPLEMENTATION · TASK STATEMENT 2.3

Implement complex hybrid and multi-account DNS architectures

Resolve, forward, sign, observe



1 Select answers and destinations

Use **split horizon** for public/private answers to the same name. Alias works at the apex; CNAME does not. Latency selects low-latency Regions; geolocation maps client locations and needs a default.

2 Forward across account boundaries

Use **conditional forwarding** for hybrid suffixes; longest match wins. Associate shared rules with spoke VPCs. SGs permit TCP/UDP 53; stateless NACLs also permit return ports. Hub endpoints centralize cost and failure scope.

3 Authenticate DNS answers

DNSSEC requires a **chain of trust**: enable public-zone signing, then publish DS at the parent. Resolver validation is separate. Route 53 rotates ZSKs automatically; KSK rollover requires coordinated DS updates.

4 Observe queries and changes

Use **query logs** for DNS troubleshooting and CloudTrail for configuration audits. Configure retention explicitly. Public health checkers cannot probe private IPs; alarm-based health checks can drive private failover.

Exam traps

- **RAM rule sharing ≠ PHZ association**. Direct cross-account PHZ association requires owner authorization and VPC-owner association. Transit Gateway connectivity alone shares neither zones nor rules.
- **DNS routing is cached**: weights approximate answer shares, not request percentages. Failover requires health signals and cache expiry; lowering TTL does not invalidate answers already cached.
- **DNSSEC authenticates, not encrypts**. Zone signing without a parent DS lacks a complete trust chain. A stale DS after KSK rollover can cause validating resolvers to return SERVFAIL.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

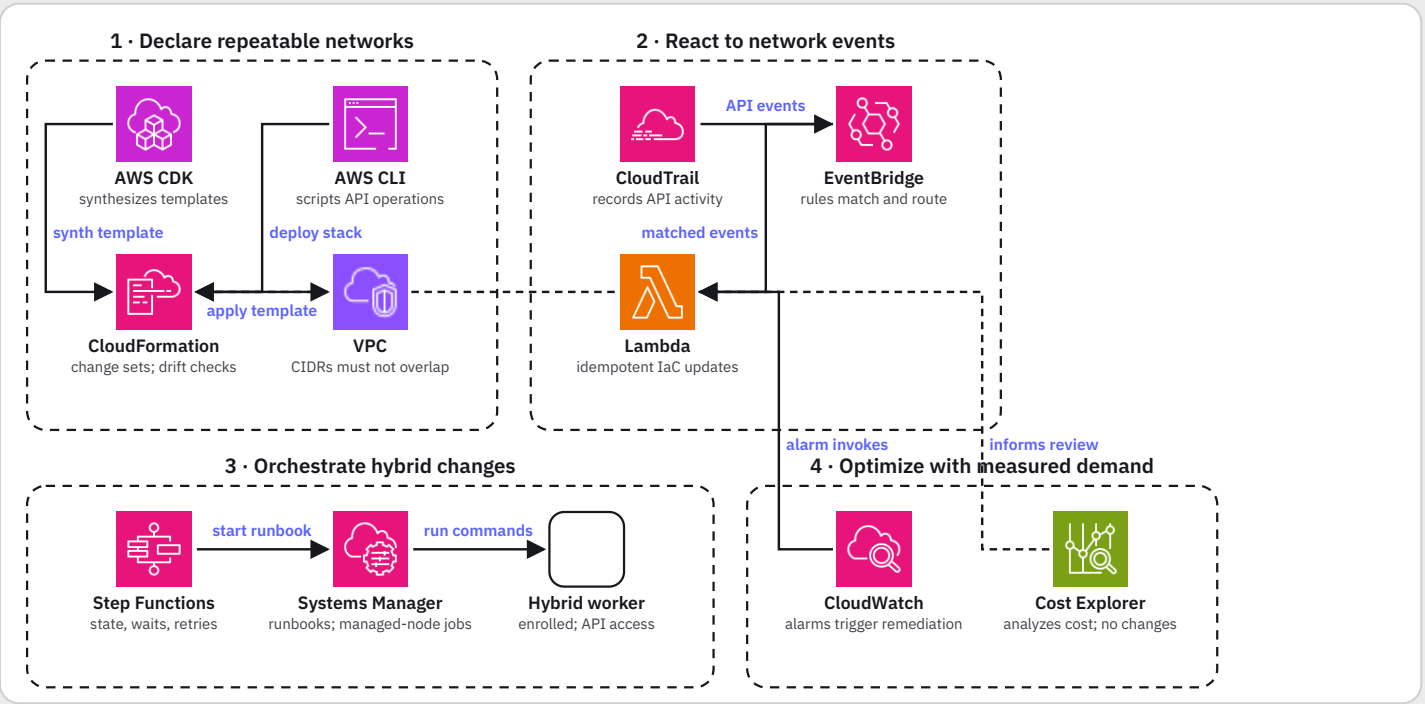
ANS-C01 · Domain 2 of 4

BlowStack

DOMAIN 2 · NETWORK IMPLEMENTATION · TASK STATEMENT 2.4

Automate and configure network infrastructure

Declare, react, orchestrate, optimize



1 Declare repeatable networks

Parameterization makes CIDRs, AZs and IDs reusable across environments; references and outputs avoid hardcoded dependencies. AWS CloudFormation manages declared state; CLI scripts alone do not provide state reconciliation.

2 React to network events

At-least-once delivery requires duplicate-safe handlers and desired-state checks. Queues buffer bursts; bounded retries with exponential backoff and jitter handle transient failures; dead-letter queues retain failed events.

3 Orchestrate hybrid changes

Hybrid automation can run device-API scripts on managed workers. AWS Direct Connect or AWS Site-to-Site VPN provides reachability, not configuration; credentials, idempotent actions and compensation remain explicit.

4 Optimize with measured demand

Measured demand drives right-sizing; cost reports do not resize resources. Alarm-driven functions can update IaC. Reviewed, staged changes reduce blast radius; lowest cost remains constrained by availability and security.

Exam traps

- **Messaging is not orchestration**: Amazon Simple Queue Service (Amazon SQS) buffers; Amazon Simple Notification Service (Amazon SNS) fans out; AWS Step Functions tracks workflow state.
- **Detection is not repair**: AWS Config evaluates compliance; AWS CloudFormation drift detection checks supported resources on request. Neither automatically restores the declared configuration.
- **Change sets preview, not guarantee safety**: AWS CloudFormation can replace network resources. Staging limits blast radius; external-device rollback requires explicit compensation.

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

AWS Certified Advanced Networking - Specialty Cheat Sheet

ANS-C01 · Domain 2 of 4

BlowStack

DOMAIN 2 · NETWORK IMPLEMENTATION · WHAT TO REMEMBER

Concepts and services of Network Implementation

Concepts to know

IP Routing

Routing selects the next hop by **longest-prefix match** before route-type tie-breakers. Connectivity requires valid forward and return paths; overlapping CIDRs prevent ordinary peering and transit routing.

Border Gateway Protocol

BGP exchanges prefixes for dynamic hybrid routing and withdraws unavailable paths. **Route preference controls failover**; AS-path prepending influences path selection, while equal-cost eligible VPN paths can support ECMP through a transit gateway.

DNS

DNS resolves names through authoritative zones and recursive resolvers. **Forwarding follows the namespace**: send corporate queries toward on-premises DNS and private AWS queries toward inbound resolver endpoints; private hosted zones require VPC association.

Core services



AWS Transit Gateway

Use for **transitive hub-and-spoke routing**. An attachment associates with one route table but can propagate into several; separate tables enforce segmentation. Inter-Region peering uses static routes.



Amazon Route 53

Use **inbound endpoints for queries entering AWS** and outbound endpoints with forwarding rules for queries leaving AWS. A matching private hosted zone returns NXDOMAIN for absent names, not public fallback.



AWS Direct Connect

Choose a **private VIF for a virtual private gateway**, a transit VIF for transit gateways through a Direct Connect gateway, or a public VIF for AWS public endpoints. The connection is not encrypted by default.

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