Networking and Content Delivery

01 MUST KNOW

if you remember five things, remember these

01 **VPC scoping:** a VPC is a **logically isolated** section of the AWS Cloud, belongs to **one Region**, and can span **multiple Availability Zones**. Each **subnet** belongs to exactly **one AZ** and is classified public (direct internet access) or private (none).

02 **CIDR rules:** a VPC's IPv4 CIDR block runs from **/16** (65,536 addresses, largest) to **/28** (16, smallest), **cannot be changed after creation**, and subnet CIDRs cannot overlap. AWS **reserves 5 addresses** in every subnet — a /24 leaves **251** usable.

03 **SG vs network ACL:** security groups work at the **instance** level, are **stateful**, support **allow rules only**, and evaluate **all rules** before deciding. Network ACLs work at the **subnet** level, are **stateless**, support **allow and deny**, and evaluate rules in **number order** (lowest first).

04 **Public vs private routing:** a subnet is public when its route table sends `0.0.0.0/0` to an **internet gateway**. Private instances reach the internet **outbound-only** through a **NAT gateway**, which must sit in a **public subnet** with an **Elastic IP**.

05 **Route 53 + CloudFront:** Route 53 is a highly available, scalable **DNS** service (names → IP addresses) with **seven routing policies**, health checks, and DNS failover. CloudFront is a **CDN** that delivers content from **edge locations** and **Regional edge caches**, pay-as-you-go.

02 KEY TERMS

TERM	DEFINITION
CIDR	IP-range notation: first address + `/n` = how many leading bits are fixed. `192.0.2.0/24` → last 8 bits flexible → 256 addresses
VPC	Your own virtual network in AWS — logically isolated, dedicated to your account, one Region, spans AZs
Subnet	A range of IP addresses dividing a VPC; lives in one AZ; public or private
Route table	Set of routes (destination → target) controlling a subnet's traffic; every table has an undeletable **local** route
Internet gateway	Scalable, redundant VPC component connecting the VPC to the internet; also does NAT for public IPv4 instances
NAT gateway	Managed NAT letting private-subnet instances reach out to the internet while blocking inbound connections
Elastic IP address	Static public IPv4 tied to your account; remap between instances anytime; extra costs can apply
Elastic network interface	Virtual NIC you can detach and reattach to another instance; its attributes follow it
VPC peering	Private routing between two VPCs (cross-account, cross-Region); non-transitive; no overlapping IPs
VPC endpoint	Private connection to supported AWS services — **interface** (PrivateLink, billed) or **gateway** (S3, DynamoDB — free)
AWS Transit Gateway	Hub-and-spoke router: each VPC / data center connects once to the hub instead of point-to-point to everything
Edge location	CloudFront data center that serves popular content to viewers at lowest latency

03 SECURITY GROUPS VS NETWORK ACLS

the module's core comparison — memorize all four rows

SECURITY GROUP	NETWORK ACL
firewall around the instance	*firewall around the subnet*
— **Instance** level — each instance can have its own set	— **Subnet** level — every subnet has exactly one
— **Stateful** — return traffic auto-allowed both ways	— **Stateless** — return traffic needs explicit rules
— **Allow** rules only — no deny	— **Allow and deny** rules
— **All rules** evaluated before the decision	— Evaluated in **number order**, lowest first (max 32,766)
— Default SG: deny all inbound · allow all outbound	— Default nACL: allow all · custom nACL: deny all until you add rules

04 CIDR ARITHMETIC WORTH MEMORIZING

fixed bits left of the slash; the rest are flexible

NOTATION	ADDRESSES	WHY IT MATTERS
/16	65,536	Largest allowed VPC IPv4 CIDR block
/24	256	As a subnet: only **251 usable** — AWS reserves 5 (network, VPC router, DNS, future use, broadcast)
/28	16	Smallest allowed VPC IPv4 CIDR block
/32	1	Every bit fixed = a single host — e.g. a firewall rule for one machine
0.0.0.0/0	all	Every bit flexible = **the internet**; destination of default routes to IGW / NAT gateway

05 VPC CONNECTIVITY OPTIONS

know each option's one-line job

OPTION	CONNECTS YOUR VPC TO…	REMEMBER
Internet gateway	The internet	Route target + NAT for public IPv4 instances
NAT gateway	Internet, outbound-only, for private subnets	Needs public subnet + Elastic IP; preferred over NAT instance
VPC endpoint	Supported AWS services, privately	Interface = PrivateLink, billed · Gateway = S3/DynamoDB, no extra charge
VPC peering	Another VPC	No overlap · not transitive · one peering per VPC pair
VPC sharing	Other accounts in your AWS Organization	Owner shares subnets; participants launch resources into them
Site-to-Site VPN	Remote network over encrypted VPN	VPN gateway (AWS side) + customer gateway (your side)
Direct Connect (DX)	Remote network via dedicated private line	Lower cost, more bandwidth, consistent; 802.1q VLANs
Transit Gateway	Many VPCs + on-premises, via one hub	Hub-and-spoke replaces point-to-point mesh

06 ROUTE 53 ROUTING POLICIES

seven policies — match the scenario to the policy

POLICY	USE WHEN…
Simple	One resource serves the function (single-server environments)
Weighted round robin	Split traffic by proportions you set (weights 0–255) — A/B testing; weights 3:1 → 75% / 25%
Latency	Resources in multiple Regions — route to the lowest **measured latency**
Geolocation	Route by **user** location — localize content, honor distribution rights

POLICY	USE WHEN…
Geoproximity	Route by **resource** location; optionally shift traffic between locations
Failover	Active-passive: health checks detect an outage and send users to the backup site
Multivalue answer	Return up to **8 healthy records** at random — helps availability, not a load-balancer substitute

07 CLOUDFRONT: INFRASTRUCTURE & PRICING

CDN = globally distributed caching servers

ITEM	FACTS
Edge location	Data centers serving **popular** content at lowest latency to viewers
Regional edge cache	Sits **between origin and edge locations**; larger cache; holds **less-popular** objects longer
Data transfer out	Charged per GB from edge to internet or to your origin; tiered by geography
HTTP(S) requests	Charged per request made to CloudFront
Invalidation requests	First **1,000 paths/month free**, then $0.005 per path
Dedicated IP custom SSL	**$600/month** per certificate, prorated hourly (1 day ≈ $20)

08 EXAM TRAPS

where the knowledge check gets you

- × “A VPC can span multiple Regions.” — **False.** A VPC belongs to one Region (spanning AZs); each subnet is confined to a single AZ.
- × “You can resize the VPC CIDR block later.” — You **cannot change** the address range after creation; choose it carefully up front.
- × “A /24 subnet gives you 256 usable addresses.” — Only **251**. AWS reserves 5: network address, VPC local router, DNS, future use, broadcast.
- × “Security groups can deny specific traffic.” — Security groups support **allow rules only**; to deny, use a **network ACL**.
- × “Network ACLs are stateful like security groups.” — nACLs are **stateless**: return traffic must be explicitly allowed, and rules fire in number order, lowest first.
- × “Defaults behave the same for both firewalls.” — The **default SG** denies all inbound / allows all outbound; the **default nACL allows everything**; a **custom nACL denies everything** until you add rules.
- × “VPC peering is transitive.” — A↔B and A↔C does **not** connect B↔C — peer them explicitly. Also: IP ranges can't overlap, and only one peering per VPC pair.
- × “A NAT gateway lets the internet reach my private instances.” — NAT is **outbound-only**: private instances can initiate connections out, but the internet cannot initiate connections in.

09 SELF-QUIZ

answers are upside-down below

Q1 Sample CCP exam: which AWS networking service enables a company to create a virtual network within AWS — AWS Config, Amazon Route 53, AWS Direct Connect, or Amazon VPC?

Q2 A VPC belongs to how many Regions, and how many Availability Zones can it span?

Q3 What are the largest and smallest IPv4 CIDR blocks allowed for a VPC?

Q4 How many addresses does AWS reserve in every subnet CIDR block, and name two of their uses.

Q5 Which VPC firewall layer is stateful, and which is stateless?

Q6 What two things must you specify when creating a NAT gateway?

Q7 To make a subnet public, what do you attach to the VPC and what route do you add?

Q8 Which Route 53 routing policy answers queries with up to eight healthy records selected at random?

Q9 Gateway VPC endpoints support exactly which two AWS services?

Q10 In CloudFront, where does content live when it is not popular enough to stay at an edge location?

ANSWER KEY (rotate the page)

Q1 Amazon VPC **Q2** one Region; multiple AZs **Q3** /16 largest, /28 smallest **Q4** five — network address, VPC local router, DNS, future use, broadcast **Q5** security groups stateful; network ACLs stateless **Q6** the public subnet it lives in and an Elastic IP address **Q7** attach an internet gateway; add route 0.0.0.0/0 → IGW **Q8** multivalue answer routing **Q9** Amazon S3 and DynamoDB **Q10** a Regional edge cache