AWS VPC Networking: Complete Architecture Guide

Interview Preparation - VPC, Subnets, Gateways, Security & Routing

1. Amazon VPC (Virtual Private Cloud) - Your Private Network in AWS

Definition: Amazon VPC is a logically isolated virtual network within AWS where you launch your resources. It's like having your own private data center in the cloud with complete control over IP addressing, subnets, routing, and security.

Concrete Example: E-commerce Application VPC

- **VPC CIDR:** 10.0.0.0/16 (65,536 IP addresses)
- **Region:** ap-south-1 (Mumbai)
- **Purpose:** Host web servers, application servers, and databases

Key VPC Characteristics:

- **Isolated:** Completely isolated from other VPCs and AWS accounts
- **Regional:** VPC spans all Availability Zones in a region
- **CIDR Block:** You define the IP address range (e.g., 10.0.0.0/16, 172.31.0.0/16)
- **Default VPC:** Every AWS account has a default VPC (172.31.0.0/16) in each region
- **Custom VPC:** You can create up to 5 VPCs per region (soft limit, can be increased)

2. Subnets - Dividing Your VPC into Smaller Networks

Definition: A subnet is a range of IP addresses within your VPC. Subnets reside in a single Availability Zone and allow you to group resources based on security and operational needs.

Types of Subnets:

Subnet Type	Internet Access	Route to IGW	Use Case	Example CIDR
Public Subnet	Yes (via IGW)	Yes (0.0.0.0/0 → IGW)	Web servers, Load balancers, NAT Gateway	10.0.1.0/24
Private Subnet	No direct access	No (uses NAT for outbound)	App servers, Databases, Internal services	10.0.2.0/24

Subnet Example (E-commerce VPC):

Real-World Analogy: Corporate Office Building Network

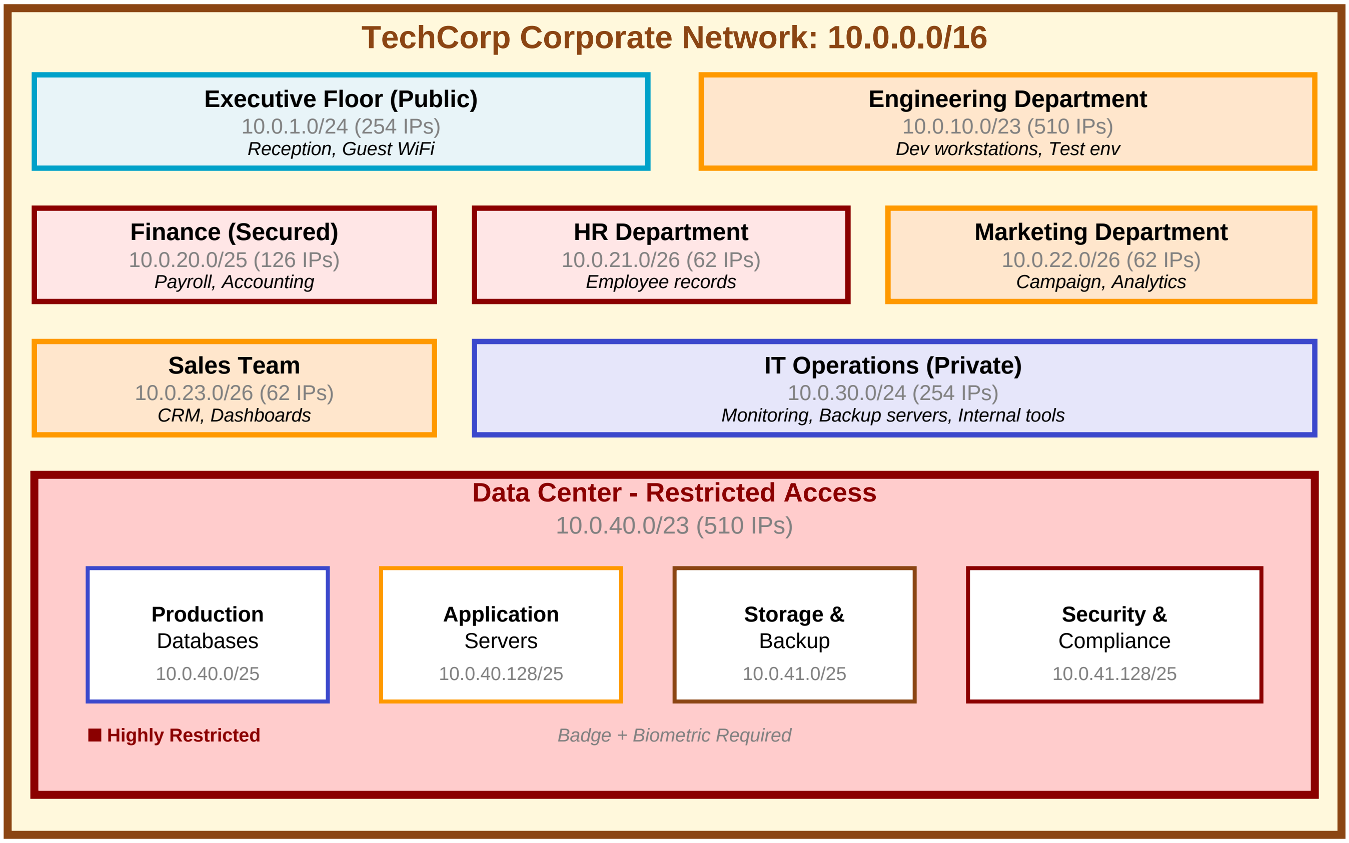
Imagine a large corporate office building (the VPC) with a total address space of 10.0.0.0/16 (65,536 IP addresses). The IT department divides this into smaller subnets for each department:

Department	Subnet CIDR	IP Range	IPs	Purpose
Executive Floor (Public)	10.0.1.0/24	10.0.1.1 - 10.0.1.254	254	Reception, Guest WiFi, Public services
Engineering	10.0.10.0/23	10.0.10.1 - 10.0.11.254	510	Dev workstations, Test environments
Finance (Secured)	10.0.20.0/25	10.0.20.1 - 10.0.20.126	126	Accounting, Payroll databases
HR Dept	10.0.21.0/26	10.0.21.1 - 10.0.21.62	62	Employee records, Recruitment
Marketing	10.0.22.0/26	10.0.22.1 - 10.0.22.62	62	Campaigns, Analytics tools
Sales Team	10.0.23.0/26	10.0.23.1 - 10.0.23.62	62	CRM systems, Dashboards
IT Operations (Private)	10.0.30.0/24	10.0.30.1 - 10.0.30.254	254	Monitoring, Backup, Internal tools
Data Center (Restricted)	10.0.40.0/23	10.0.40.1 - 10.0.41.254	510	Prod databases, Core infrastructure

Key Points from Company Network Example:

- **Segmentation:** Each department isolated in its own subnet for security and management
- **Variable Sizes:** Engineering gets /23 (512 IPs), HR gets /26 (64 IPs) based on needs
- **Access Control:** Finance subnet restricted, Executive floor more open
- **Hierarchical:** 10.0.0.0/16 (company) → 10.0.10.0/23 (engineering) → individual devices

Visual: Company Building Network Layout



Color Code: Blue=Public Access | Orange=Standard Access | Red=Restricted Access | Purple=IT Only

How This Maps to AWS VPC Subnets:

- **Executive Floor (Public) → AWS Public Subnet:** Internet-facing, accessible from outside
- **Departments (Private) → AWS Private Subnets:** Internal access only, isolated from internet
- **Data Center (Restricted) → AWS Private DB Subnet:** Highly secured, no internet access
- **IT Operations → AWS Management Subnet:** Monitoring, logging, administrative tools

Now Let's Apply This to AWS E-commerce VPC:

Subnet Name	CIDR Block	AZ	Type	Resources
Public-AZ-A	10.0.1.0/24	ap-south-1a	Public	ALB, NAT Gateway
Private-App-AZ-A	10.0.2.0/24	ap-south-1a	Private	EC2 App Servers
Private-DB-AZ-A	10.0.3.0/24	ap-south-1a	Private	RDS Primary
Public-AZ-B	10.0.11.0/24	ap-south-1b	Public	ALB, NAT Gateway
Private-App-AZ-B	10.0.12.0/24	ap-south-1b	Private	EC2 App Servers
Private-DB-AZ-B	10.0.13.0/24	ap-south-1b	Private	RDS Standby

Key Subnet Concepts:

- **One AZ Only:** Each subnet exists in exactly one Availability Zone

- **Reserved IPs:** AWS reserves 5 IPs in each subnet (.0, .1, .2, .3, .255)
- **Subnet Mask:** /24 gives 256 IPs (251 usable), /16 gives 65,536 IPs
- **High Availability:** Deploy across multiple AZs for fault tolerance

CIDR Notation Reference Chart - Quick Subnet Calculator

Understanding CIDR (Classless Inter-Domain Routing): The number after the slash (/) indicates how many bits are used for the network portion. The remaining bits are for host addresses.

Common CIDR Blocks for AWS Subnets:

Prefix	Subnet Mask	Total IPs	Usable IPs	Common Use in AWS
/32	255.255.255.255	1	1	Single host (EIP, specific instance)
/31	255.255.255.254	2	2	Point-to-point links
/30	255.255.255.252	4	2	Very small networks
/29	255.255.255.248	8	3	Tiny subnets
/28	255.255.255.240	16	11	Small Lambda VPC subnets
/27	255.255.255.224	32	27	Small application subnets
/26	255.255.255.192	64	59	Small department subnets
/25	255.255.255.128	128	123	Medium subnets
/24	255.255.255.0	256	251	★ Most common subnet size
/23	255.255.254.0	512	507	Larger department subnets
/22	255.255.252.0	1,024	1,019	Large application tier
/21	255.255.248.0	2,048	2,043	Very large subnets
/20	255.255.240.0	4,096	4,091	Large-scale deployments

Larger CIDR Blocks (VPC-level):

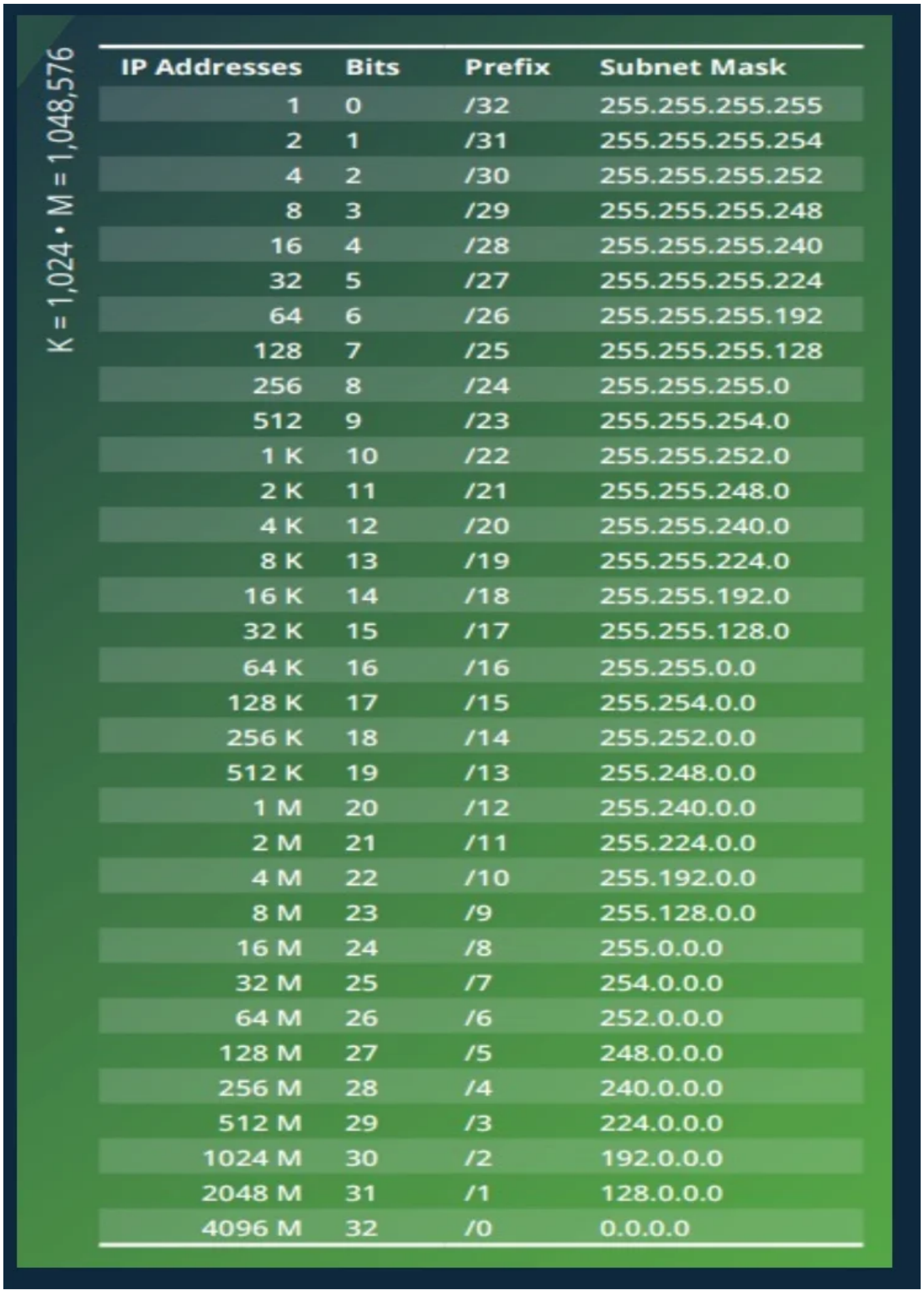
Prefix	Subnet Mask	Total IPs	Usable IPs	Common Use in AWS
/19	255.255.224.0	8,192	8,187	Very large subnet
/18	255.255.192.0	16,384	16,379	Large VPC segment
/17	255.255.128.0	32,768	32,763	Half of /16 VPC
/16	255.255.0.0	65,536	65,531	★ Common VPC size
/15	255.254.0.0	131,072	131,067	Very large VPC
/14	255.252.0.0	262,144	262,139	Huge enterprise VPC
/13	255.248.0.0	524,288	524,283	Massive VPC
/12	255.240.0.0	1,048,576	1,048,571	Maximum usable VPC
/11	255.224.0.0	2,097,152	2,097,147	Beyond AWS limits
/10	255.192.0.0	4,194,304	4,194,299	Theoretical only

Important Notes:

- **AWS Reserves 5 IPs:** First 4 (.0, .1, .2, .3) and last (.255) - so /24 gives 251 usable, not 256
- **VPC CIDR Range:** Minimum /28 (16 IPs), Maximum /16 (65,536 IPs)
- **Common Pattern:** VPC /16, Subnets /24 (gives 256 subnets per VPC)
- **Formula:** Usable IPs = 2^(32-prefix) - 5 (for AWS subnets)

Complete CIDR Reference Chart:

Below is a comprehensive CIDR notation chart showing all possible subnet sizes from /0 to /32:



K = 1,024 • M = 1,048,576

IP Addresses	Bits	Prefix	Subnet Mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1 K	10	/22	255.255.252.0
2 K	11	/21	255.255.248.0
4 K	12	/20	255.255.240.0
8 K	13	/19	255.255.224.0
16 K	14	/18	255.255.192.0
32 K	15	/17	255.255.128.0
64 K	16	/16	255.255.0.0
128 K	17	/15	255.254.0.0
256 K	18	/14	255.252.0.0
512 K	19	/13	255.248.0.0
1 M	20	/12	255.240.0.0
2 M	21	/11	255.224.0.0
4 M	22	/10	255.192.0.0
8 M	23	/9	255.128.0.0
16 M	24	/8	255.0.0.0
32 M	25	/7	254.0.0.0
64 M	26	/6	252.0.0.0
128 M	27	/5	248.0.0.0
256 M	28	/4	240.0.0.0
512 M	29	/3	224.0.0.0
1024 M	30	/2	192.0.0.0
2048 M	31	/1	128.0.0.0
4096 M	32	/0	0.0.0.0

Quick CIDR Calculation Tips for Interviews:

- **/24 = 256 IPs:** Easy to remember, most common subnet
- **/25 = 128 IPs:** Half of /24
- **/23 = 512 IPs:** Double of /24
- **/16 = 65,536 IPs:** Standard VPC size
- **Each -1 in prefix = Double the IPs:** /23 has 2x more IPs than /24
- **Each +1 in prefix = Half the IPs:** /25 has half the IPs of /24

3. Internet Gateway (IGW) - Connect VPC to the Internet

Definition: An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.

Internet Gateway Characteristics:

- **One IGW per VPC:** Each VPC can have only one Internet Gateway attached
- **Highly Available:** Managed by AWS, no single point of failure
- **No Bandwidth Limits:** Automatically scales based on traffic
- **Stateless:** Does not track connection state (unlike NAT Gateway)
- **Two Functions:** Provides route target for internet traffic + performs NAT for public IPs

How IGW Works:

Step	Process	Example
1	EC2 has private IP (10.0.1.5) and public IP (13.232.45.67)	Instance in public subnet
2	Instance sends packet with source: 10.0.1.5, dest: 8.8.8.8	Trying to reach Google DNS
3	Route table directs 0.0.0.0/0 traffic to IGW	All internet traffic → IGW
4	IGW performs NAT: replaces 10.0.1.5 with 13.232.45.67	Source becomes public IP
5	Packet leaves AWS to internet with public IP	Internet sees 13.232.45.67
6	Response comes back to 13.232.45.67	Reply from 8.8.8.8
7	IGW translates back: 13.232.45.67 → 10.0.1.5	Delivered to instance

4. Route Tables - Controlling Traffic Flow in VPC

Definition: A route table contains rules (routes) that determine where network traffic from your subnet or gateway is directed. Every subnet must be associated with a route table.

Route Table Types:

- **Main Route Table:** Default table automatically created with VPC
- **Custom Route Tables:** Additional tables you create for specific routing needs
- **Subnet Association:** Each subnet uses one route table (main or custom)

Example Route Tables:

Public Subnet Route Table:

Destination	Target	Meaning
10.0.0.0/16	local	All VPC internal traffic stays within VPC
0.0.0.0/0	igw-12345abc	All internet traffic goes to Internet Gateway

Private Subnet Route Table:

Destination	Target	Meaning
10.0.0.0/16	local	All VPC internal traffic stays within VPC
0.0.0.0/0	nat-0987xyz	All internet traffic goes to NAT Gateway (for outbound only)

Route Selection Logic:

- **Most Specific Match:** Longest prefix match wins (e.g., 10.0.1.0/24 beats 10.0.0.0/16)
- **Local Always First:** VPC CIDR (local) routes have highest priority
- **Default Route:** 0.0.0.0/0 is the catch-all for any destination not explicitly matched

5. NAT Gateway - Enabling Outbound Internet for Private Subnets

Definition: A NAT (Network Address Translation) Gateway allows instances in private subnets to connect to the internet for outbound traffic (e.g., software updates) while preventing inbound connections from the internet.

NAT Gateway vs NAT Instance:

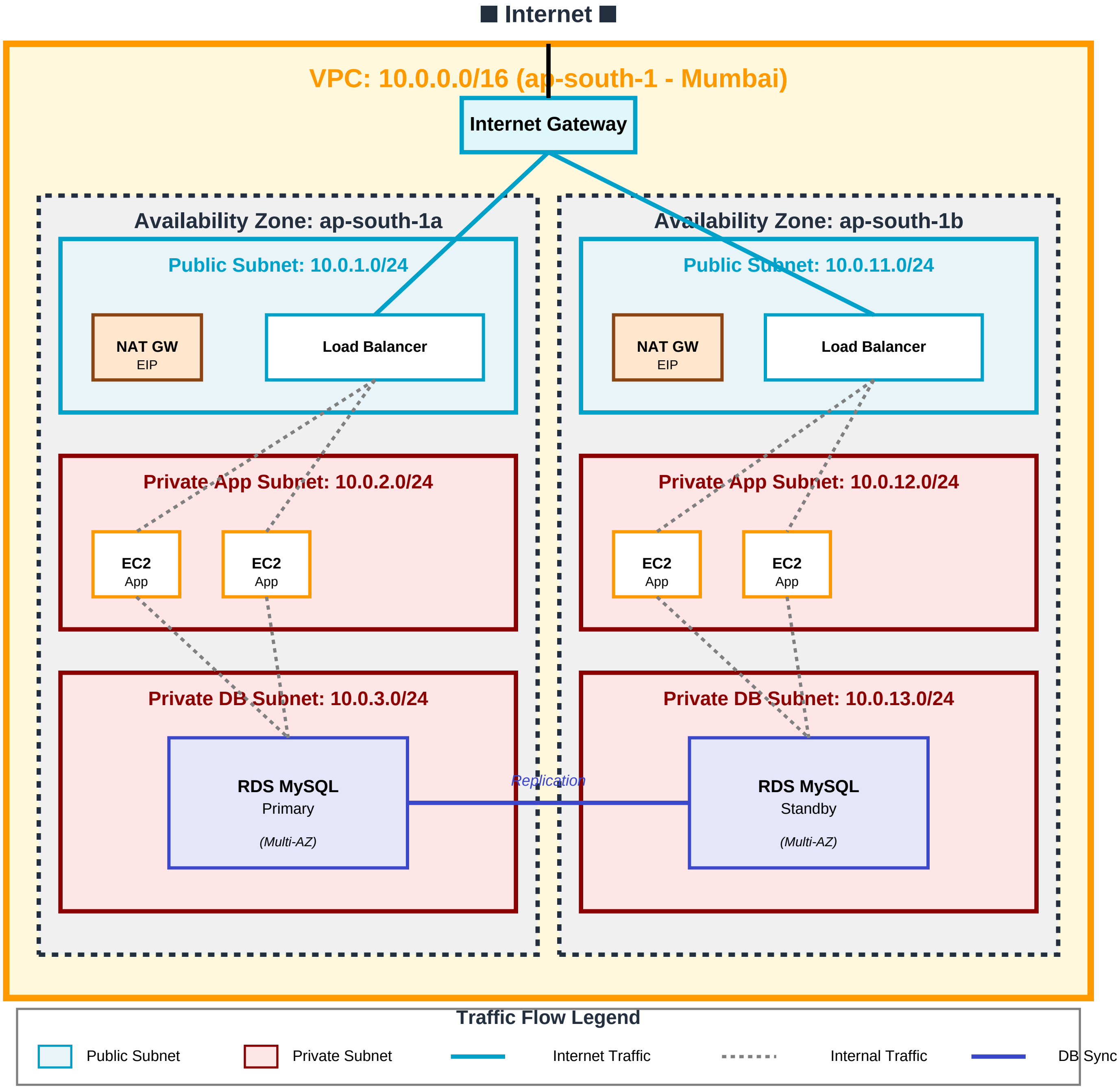
Aspect	NAT Gateway (Managed)	NAT Instance (DIY)
Availability	Highly available within AZ (AWS managed)	Use scripts for failover between instances
Bandwidth	Scales up to 100 Gbps	Depends on EC2 instance type

Maintenance	Managed by AWS	You manage updates, patches, failures
Cost	$0.045/hour + $0.045/GB processed	EC2 instance cost + data transfer
Performance	Optimized by AWS	Depends on instance type and config
Security Groups	Not supported (uses NACLs only)	Supported
Use as Bastion	No	Can configure as bastion host

NAT Gateway Key Points:

- **Public Subnet:** NAT Gateway must be in a public subnet
- **Elastic IP:** Requires an Elastic IP (static public IP)
- **One per AZ:** For HA, deploy one NAT Gateway per AZ
- **Outbound Only:** Allows private instances to initiate outbound connections only
- **Stateful:** Tracks connections, return traffic automatically allowed

6. Complete VPC Architecture Diagram


■ Internet ■
VPC: 10.0.0.0/16 (ap-south-1 - Mumbai)
Internet Gateway
Availability Zone: ap-south-1a
Public Subnet: 10.0.1.0/24
NAT GW
EIP
Load Balancer
Private App Subnet: 10.0.2.0/24
EC2
App
EC2
App
Private DB Subnet: 10.0.3.0/24
RDS MySQL
Primary
(Multi-AZ)
Replication
Availability Zone: ap-south-1b
Public Subnet: 10.0.11.0/24
NAT GW
EIP
Load Balancer
Private App Subnet: 10.0.12.0/24
EC2
App
EC2
App
Private DB Subnet: 10.0.13.0/24
RDS MySQL
Standby
(Multi-AZ)
Traffic Flow Legend
Public Subnet
Private Subnet
Internet Traffic
Internal Traffic
DB Sync

Key Architecture Points:

- **Multi-AZ Design:** Resources deployed across 2 AZs for high availability
- **Public Subnets:** Host ALB and NAT Gateways with route to Internet Gateway
- **Private Subnets:** App and DB tiers isolated from direct internet access
- **NAT Gateway per AZ:** Enables private instances to download updates
- **Database Replication:** RDS Multi-AZ with synchronous replication

7. Security Groups - Instance-Level Firewall (Stateful)

Definition: Security Groups act as virtual firewalls at the instance level (ENI - Elastic Network Interface). They control inbound and outbound traffic using ALLOW rules only. Security Groups are STATEFUL - return traffic is automatically allowed.

Security Group Characteristics:

- **Stateful:** If you allow inbound request, response is automatically allowed
- **Allow Rules Only:** You can only specify ALLOW rules, not DENY rules
- **Instance Level:** Applied to ENI (network interface) of EC2, RDS, Lambda, etc.
- **Multiple Groups:** You can assign up to 5 security groups per instance
- **Default Deny:** All inbound traffic denied by default, all outbound allowed

Example Security Groups (E-commerce App):

1. ALB Security Group (alb-sg):

Type	Protocol	Port	Source	Description
Inbound	HTTP	80	0.0.0.0/0	Allow HTTP from anywhere
Inbound	HTTPS	443	0.0.0.0/0	Allow HTTPS from anywhere
Outbound	ALL	ALL	app-tier-sg	Forward to app servers

2. App Tier Security Group (app-tier-sg):

Type	Protocol	Port	Source	Description
Inbound	HTTP	8080	alb-sg	Allow traffic from ALB only
Inbound	SSH	22	bastion-sg	SSH access from bastion host
Outbound	MySQL	3306	db-sg	Connect to database
Outbound	HTTPS	443	0.0.0.0/0	Download updates, API calls

3. Database Security Group (db-sg):

Type	Protocol	Port	Source	Description
Inbound	MySQL	3306	app-tier-sg	Allow from app tier only
Outbound	ALL	ALL	0.0.0.0/0	Default (rarely used)

Security Group Best Practices:

- **Least Privilege:** Only open ports that are absolutely necessary
- **Reference Other SGs:** Use security group IDs as source (e.g., app-tier-sg → db-sg)
- **No 0.0.0.0/0 for SSH:** Never allow SSH from anywhere, use bastion or VPN
- **Separate SGs per Tier:** ALB, App, Database should have different security groups

8. Network ACLs (NACLs) - Subnet-Level Firewall (Stateless)

Definition: Network Access Control Lists (NACLs) are stateless firewalls that control traffic at the subnet level. Unlike Security Groups, NACLs support both ALLOW and DENY rules and are processed in rule number order.

NACL Characteristics:

- **Stateless:** You must explicitly allow both inbound AND outbound traffic
- **Subnet Level:** Applied to entire subnet, affects all instances in that subnet
- **ALLOW and DENY:** Can create both allow and deny rules
- **Rule Numbers:** Rules evaluated in order (100, 200, 300...), lowest first
- **Default NACL:** Allows all inbound and outbound traffic
- **Custom NACL:** Denies all traffic by default until you add rules

Example NACL (Public Subnet):

Inbound Rules:

Rule #	Type	Protocol	Port	Source	Allow/Deny
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	203.0.113.0/24	ALLOW
130	Ephemeral	TCP	1024-65535	0.0.0.0/0	ALLOW
*	ALL	ALL	ALL	0.0.0.0/0	DENY

Outbound Rules:

Rule #	Type	Protocol	Port	Destination	Allow/Deny
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	Ephemeral	TCP	1024-65535	0.0.0.0/0	ALLOW
*	ALL	ALL	ALL	0.0.0.0/0	DENY

Important NACL Notes:

- **Ephemeral Ports:** Must allow ephemeral ports (1024-65535) for return traffic
- **Stateless:** Must define both inbound and outbound rules explicitly
- **Rule Order:** First matching rule wins, * rule is catch-all deny
- **Block Specific IPs:** Use DENY rules to block malicious IPs (Security Groups can't)

9. Security Groups vs Network ACLs - Key Differences

Aspect	Security Group	Network ACL
Level	Instance (ENI) level	Subnet level
State	Stateful (return traffic auto-allowed)	Stateless (must allow both directions)
Rules	ALLOW rules only	ALLOW and DENY rules
Rule Processing	All rules evaluated	Rules processed in order (by rule #)
Application	Applied to specific instances	Applies to ALL instances in subnet
Default Behavior	Deny all inbound, allow all outbound	Default NACL: Allow all Custom NACL: Deny all
Use Case	Granular instance-level security	Subnet-level defense, block IPs
Number of Groups/ACLs	Up to 5 per instance	One NACL per subnet

When to Use Which?

Use Security Groups when:

- You need instance-specific firewall rules
- You want to reference other security groups as source/destination
- You need stateful filtering (most common use case)

Use Network ACLs when:

- You need to block specific IP addresses (DENY rules)
- You want subnet-level protection as an additional security layer
- Compliance requires stateless filtering

Best Practice: *Use Security Groups as primary security control. Use NACLs as an additional layer of defense for subnet-level protection and to block malicious IPs.*

10. Public Subnet vs Private Subnet - Complete Summary

Aspect	Public Subnet	Private Subnet
Internet Access	Direct internet access via IGW	No direct access (uses NAT for outbound)

Route Table	Has route: 0.0.0.0/0 → IGW	Has route: 0.0.0.0/0 → NAT Gateway (optional)
Public IP	Instances can have public IPs	Instances have private IPs only
Inbound from Internet	Yes (if Security Group allows)	No (isolated from internet)
Outbound to Internet	Yes (direct via IGW)	Yes (via NAT Gateway in public subnet)
Typical Resources	• Load Balancers (ALB/NLB) • NAT Gateway • Bastion Host • VPN Server	• Application Servers • Databases (RDS) • Lambda functions • ElastiCache
Security Posture	More exposed, requires strict SGs	More secure, isolated from direct internet
Cost	Data transfer costs to/from internet	Data transfer + NAT Gateway costs

11. Interview Key Points to Remember

When explaining VPC:

- VPC = Isolated virtual network in AWS with your own IP range (CIDR)
- Regional resource that spans all AZs
- Use concrete example: 10.0.0.0/16 for e-commerce app in Mumbai

When explaining Subnets:

- Subnet = Segment of VPC in a single AZ
- Public subnet has route to Internet Gateway (0.0.0.0/0 → IGW)
- Private subnet uses NAT Gateway for outbound-only internet access
- AWS reserves 5 IPs per subnet (.0, .1, .2, .3, .255)

When explaining Internet Gateway:

- One IGW per VPC, horizontally scaled by AWS
- Performs NAT for instances with public IPs
- Stateless, no bandwidth limit

When explaining Route Tables:

- Every subnet must have a route table
- Local route (VPC CIDR) always has priority
- 0.0.0.0/0 is default route (catch-all)
- Most specific route wins (longest prefix match)

When explaining NAT Gateway:

- Enables private instances to access internet (outbound only)
- Must be in public subnet with Elastic IP
- Managed service (vs NAT instance which is DIY)
- Deploy one per AZ for high availability

When explaining Security Groups:

- Instance-level firewall, STATEFUL
- ALLOW rules only, no DENY rules
- Return traffic automatically allowed
- Can reference other security groups (e.g., app-sg → db-sg)

When explaining NACLs:

- Subnet-level firewall, STATELESS
- Both ALLOW and DENY rules supported
- Must explicitly allow both inbound and outbound
- Rules processed in order by rule number

- Use for blocking specific IPs (Security Groups can't deny)

12. Common Interview Questions & Answers

Question	Answer
What makes a subnet public?	Route table has 0.0.0.0/0 → Internet Gateway AND instance has public IP
Can private subnet access internet?	Yes, for outbound only via NAT Gateway in public subnet
Security Group vs NACL?	SG: Stateful, instance-level, ALLOW only NACL: Stateless, subnet-level, ALLOW + DENY
Why use NAT Gateway over NAT Instance?	Managed by AWS, highly available, scales to 100 Gbps, no maintenance
How many IGWs per VPC?	Exactly ONE Internet Gateway per VPC
What are ephemeral ports?	Temporary ports (1024-65535) used for return traffic in NACL outbound rules
VPC peering vs Transit Gateway?	Peering: 1-to-1 connection Transit Gateway: Hub for multiple VPCs/on-prem