2025

CYBERSECURITY INTERVIEW QUESTIONS STUDY GUIDE

DAVID BAPTIST

TABLE OF CONTENTS

Networking fundamentals and deep subnetting 3

Subnetting deep dive 4

- Masks and increments table 5
- Worked examples 5
- Binary method in one minute 6
- Design guidelines 6
- IPv6 crash course for interviews 6
- Quick practice with answers 7

Endpoint security and malware 7

Operating system security 9

Cryptography and PKI 10

Cloud security 11

Governance, risk, and compliance with RMF and POA and M 12

Incident response and threat hunting 14

Vulnerability management and penetration testing 15

Security architecture and Zero Trust 16

DevSecOps and automation 17

Secure SDLC and threat modeling 18

General software development fundamentals 19

Top 20 rapid fire interview Q and A 21

Cheat sheets and quick reference 23

- OSI model 23
- Common ports 23
- Subnet quick chart 24

Windows event ids to memorize 24

Linux quick commands 25

Fast subnet practice with answers *25*

Extra networking study block *25*

NAT types **25**

ACL tips **25**

DNS security reminders **26**

Closing tip *26*

NETWORKING FUNDAMENTALS AND DEEP SUBNETTING

QUESTION 1. STATEFUL VS STATELESS FIREWALL

A stateful firewall tracks connection state such as the TCP handshake and keeps a session table. It can allow return traffic dynamically. A stateless firewall evaluates each packet against static rules only. For enterprise networks I prefer stateful at aggregation and stateless for very high-speed edge filtering.

Notes

• Stateful uses connection tables and sequence awareness

• Stateless is faster and simpler and is often used as an initial packet filter or in cloud service provider network ACLs

QUESTION 2. IDS VS IPS

IDS monitors and alerts on suspicious traffic out of band. IPS is inline and can block in real time. Many platforms provide both by running sensors in tap or span mode for visibility and policy inline at choke points for prevention.

Notes

• Signature, behavior, and machine learning detections

• Tuning suppresses noisy rules and reduces false positives

• Place inline only where you can tolerate latency

QUESTION 3. PREVENTING MAN IN THE MIDDLE

Enforce TLS everywhere with strong cipher suites, use HSTS for web, device certificates for VPN, and port security on switches with DHCP snooping and dynamic ARP inspection. Add user and device identity checks with 802.1X.

QUESTION 4. TCP THREE-WAY HANDSHAKE

Client sends SYN, server replies to SYN ACK, client confirms with ACK. This negotiates sequence numbers and window sizes and lets stateful devices confirm a real connection. It also enables defenses like SYN cookies against floods.

QUESTION 5. SEGMENTATION AND ZERO TRUST

Start with VLAN and subnet boundaries for users, servers, and management. Enforce least privilege flows with ACLs and micro segmentation at the host or overlay level. Zero Trust layer’s identity and device health checks on every access request with default deny.

SUBNETTING DEEP DIVE

An IPv4 address is 32 bits. The subnet mask marks how many high order bits belong to the network and how many remain for hosts.

EXAMPLE

192.168.10.25 with mask 255.255.255.0 means 24 network bits and 8 host bits. The network is 192.168.10.0 and the broadcast is 192.168.10.255.

CIDR NOTATION

/x means x network bits. The rest are host bits.

CORE FORMULAS

- Total addresses per subnet = 2^ (host bits)
- Usable hosts per subnet = 2^ (host bits) minus 2
- Number of equal subnets created by borrowing n bits = 2^n

MASKS AND INCREMENTS TABLE

CIDR	Mask	Total IPs	Usable hosts	Subnet increment in last octet
/24	255.255.255.0	256	254	1
/25	255.255.255.128	128	126	128
/26	255.255.255.192	64	62	64
/27	255.255.255.224	32	30	32
/28	255.255.255.240	16	14	16
/29	255.255.255.248	8	6	8
/30	255.255.255.252	4	2	4

Subnet increment tells you where each subnet starts inside the parent. Example for a slash 26 inside a slash 24: starts at .0 .64 .128 .192

WORKED EXAMPLES

Example A. Split 192.168.10.0 slash 24 into four equal subnets

• Four equals 2 squared so borrow 2 bits which gives slash 26

• New mask 255.255.255.192

• Subnets with ranges

• 192.168.10.0 slash 26 usable .1 through .62 broadcast .63

• 192.168.10.64 slash 26 usable .65 through .126 broadcast .127

• 192.168.10.128 slash 26 usable .129 through .190 broadcast .191

• 192.168.10.192 slash 26 usable .193 through .254 broadcast .255

Example B. You need at least 50 hosts for Finance and at least 20 for HR inside 10.0.0.0 slash 24 using VLSM

• Finance needs 50 so the next power of two is 64 which is slash 26

Finance network 10.0.0.0 slash 26 usable .1 through .62

• HR needs 20 so choose 32 which is slash 27

Next free block starts at .64 with increment 32

HR network 10.0.0.64 slash 27 usable .65 through .94

• You still have .96 and above for other teams

Example C. Route summarization

Given subnets 172.16.8.0 slash 24 through 172.16.15.0 slash 24

• They share a common prefix of 172.16.8.0 to 172.16.15.255 which is a block of 8 slash 24 networks or 2048 addresses

• 8 slash 24s equals a slash 21 summary

• Summary route is 172.16.8.0 slash 21 which covers .8.0 through .15.255

BINARY METHOD IN ONE MINUTE

1. Write the interesting octet in binary

   Example for slash 26 from slash 24 we borrow two bits in the last octet

   Mask bits become 11000000 which is 192

2. Subnet starts where borrowed bits flip

   00 000000 gives .0

   01 000000 gives .64

   10 000000 gives .128

   11 000000 gives .192

DESIGN GUIDELINES

• Plan by required host counts plus growth and round up to next power of two

• Keep infrastructure addresses low to keep room for host growth

• Do not overlap subnets or summarization breaks routing

• IPv6 addresses are 128 bits written in hex with groups separated by colons

• Subnetting uses slash prefix length, and most site subnets are slash 64

• No broadcast in IPv6

• Stateless address autoconfiguration and neighbor discovery replace ARP

QUICK PRACTICE WITH ANSWERS

1. How many usable hosts in slash 20

   32 minus 20 equals 12 host bits so 2 to the 12 minus 2 equals 4094

2. First usable of 10.23.48.0 slash 27

   Increment is 32 so the block ranges are .48.0 to .48.31 .48.32 to .48.63 etc.

   First usable is 10.23.48.1

3. What block would fit exactly 6 points to point links

   Each point to point is slash 30 which has 2 usable

   Six links equal 6 times 4 addresses equal 24 addresses

   A slash 27 has 32 total and is a comfortable fit and leaves room to grow

ENDPOINT SECURITY AND MALWARE

QUESTION 1. ROOTKIT RESPONSE

Treat rootkits as a full rebuild scenario. Isolate the host, collect volatile memory and triage with your EDR, acquire a forensic image if required, then reimage from a gold baseline and rotate credentials. Post incident, close initial access and harden.

Notes

• Kernel mode rootkits subvert visibility so you cannot trust on box tools

IPV6 CRASH COURSE FOR INTERVIEWS

• Preserve chain of custody for evidence

• Golden image with current patches and baseline controls is part of recovery

QUESTION 2. SIGNATURE VERSUS BEHAVIOR DETECTION

Signatures match known patterns and are fast but brittle against variants. Behavior looks for suspicious actions such as unusual process trees or credential dumping and can catch unknowns. I run both with careful tuning and user reported phishing integrated into response.

Notes

• Add sandbox detonation for suspicious attachments

• Measure mean time to detect and mean time to contain

QUESTION 3. RANSOMWARE KILL CHAIN AND CONTAINMENT

Typical flow is phishing, or exposed RDP then credential harvest then lateral movement then encryption of shares. Contain by isolating machines, disabling malicious accounts and sessions, killing processes, and restoring from immutable backups. Use application allow lists and least privilege on shares to reduce blast radius.

QUESTION 4. SUSPICIOUS WINDOWS PROCESS INVESTIGATION

Check parent process and command line, signature and path, loaded modules, network connections, recent persistence locations, and compare to baseline. Pivot on hash and reputation and detonate in a sandbox if needed.

USEFUL WINDOWS ARTIFACTS

• Event 4688 process creation and 1 for Sysmon

• Autoruns locations such as Run keys, services, scheduled tasks, WMI

• PowerShell logs module and script block and transcription

QUESTION 5. HOW EDR ADDS VALUE

EDR collects detailed telemetry and correlates behaviors to detect attacks that bypass signatures. It also gives real time actions such as isolate host, kill process, collect memory, and pull triage packages.

OPERATING SYSTEM SECURITY

SSH HARDENING

Disable root login, require keys and preferably FIDO tokens, restrict to specific users or groups, and enforce modern ciphers. Use fail2ban or equivalent and require jump hosts for admin access.

LINUX COMMANDS

- sshd_config settings: PermitRootLogin no, PasswordAuthentication no, AllowUsers, KexAlgorithms
- sudo pam tally2 or faillock for lockouts
- auditd rules for critical files

LINUX LOGS DURING INCIDENT

- /var/log/auth.log or secure for logins
- journalctl -xe for recent system errors
- Web logs such as access log and error log
- Service and application specific logs

DAC VS MAC

Discretionary access control gives the owner power over permissions while mandatory access control enforces central policy labels such as SELinux or AppArmor to confine processes even if compromised.

WINDOWS SERVER HARDENING

Apply least privilege, remove unnecessary roles, enforce attack surface reduction rules, enable LAPS and Credential Guard, secure PowerShell with logging and constrained language, and follow a CIS baseline.

IMPORTANT WINDOWS EVENT IDS TO REMEMBER

- 4624 logon success, 4625 failure
- 4672 special privileges assigned
- 4688 process creation
- 7045 service installed
- 4720 account created, 4732 user added to group

CRYPTOGRAPHY AND PKI

SYMMETRIC VS ASYMMETRIC

Symmetric uses a shared secret and is fast for bulk data such as AES. Asymmetric uses a key pair and enables exchange and signatures like RSA or ECDSA. In TLS we use asymmetric to agree on a session key then switch to symmetric.

TLS HANDSHAKE QUICK

TLS 1.3 removes many legacy steps. The client sends supported ciphers and key shares. The server selects parameters and sends its certificate and signature. Both derive keys and switch to encrypted traffic early which provides forward secrecy.

DIGITAL SIGNATURES

Hash the message then sign the hash with the private key. Anyone with the public key can verify both integrity and authenticity.

CERTIFICATE AUTHORITIES AND TRUST

A CA validates identity and signs leaf certificates. Clients trust a root store and build a chain from the leaf through intermediates to a root. Use short lived certs and OCSP stapling to improve revocation behavior.

HASHING VS ENCRYPTION

Hashing is one way for integrity and password storage. Encryption is two way for confidentiality. Salting and stretching with modern password hashing algorithms is required for credentials.

CLOUD SECURITY

DATA AT REST AND IN TRANSIT

Use provider managed encryption with customer managed keys for storage and enforce TLS for data in transit. Log key usage, restrict key administrators, and rotate keys on schedule.

IDENTITY AND ACCESS

Use roles with least privilege and short-lived tokens instead of long-lived keys. Separate break glass and admin accounts. Review permissions and use policy guardrails at the account or subscription level.

COMPROMISED INSTANCE RESPONSE

Quarantine by removing it from load balancers or using provider isolation, snapshot disks and memory, when possible, rotate all secrets, and redeploy from known good templates. Then fix the initial access vector such as a leaked key or open security group.

SHARED RESPONSIBILITY

Provider secures the cloud. You secure what you configure and deploy including identities, data, and network controls.

PREVENT STORAGE LEAKS

Block public access at account level, require explicit policies for any public object, and continuously scan for exposure. Use object encryption and access logs.

GOVERNANCE, RISK, AND COMPLIANCE WITH RMF AND POA AND M

NIST 800 53 VS ISO 27001

NIST 800 53 is a deep control catalog used by United States federal systems and many contractors. ISO 27001 is a management system standard that focuses on risk driven governance and continual improvement. In practice I map 800 53 technical controls into an ISMS that follows ISO processes.

RMF STEPS WITH ARTIFACTS

1. Categorize the system and define boundaries and data types
2. Select controls with tailoring and overlays
3. Implement controls and document in the SSP

4. Assess controls with an SAP and produce a SAR
5. Authorize with a decision by the AO supported by the package
6. Monitor continuously with POA and M updates and ongoing assessments

COMMON ARTIFACTS

• SSP system security plan

• SAP security assessment plan

• SAR security assessment report

• POA&M plan of action and milestones

• Control implementation evidence such as configurations and scans

POA&M PURPOSE

POA and M records control gaps with owners, milestones, budgets, residual risk, and due dates. It drives remediation and makes risk acceptance explicit.

GOOD POA&M PRACTICE

• Actionable milestones with dates tied to tickets

• Clear status definitions such as open on track delayed completed

• Link evidence and approvals

• Separate risk acceptance from remediation to avoid confusion

CONTINUOUS COMPLIANCE

Automate evidence collection from tools and APIs, map detections and posture checks to controls, and generate attestation reports on schedule. Use IaC modules and policy as code to make desired state auditable.

INCIDENT RESPONSE AND THREAT HUNTING

INCIDENT RESPONSE LIFECYCLE

Prepare then detect and analyze then contain then eradicate then recover then lessons learned. Communication plans and roles are as important as tools.

INVESTIGATE ABNORMAL OUTBOUND TRAFFIC

Baseline normal destinations, review DNS and proxy logs for rare domains, pivot to the process that opened the socket, and check for staging paths such as temp directories and archive creation. Cut egress while you investigate if data loss is suspected.

ANALYST PLAYBOOK SNIPPETS

- Splunk like query: index=proxy OR index=dns rare limit=20 by domain
- KQL like query: DeviceNetworkEvents | summarize count () by RemoteUrl | top 20 by count asc
- Look for long domain labels and high entropy strings that hint at tunneling

IOC VS IOA (INDICATORS OF COMPROMISE VS INDICATORS OF ATTACK)

IOCs are specific artifacts such as hashes domains or IPs. IOAs describe behaviors like credential dumping or lateral movement that generalize better. I focus hunts on IOAs and use IOCs as enrichment.

PRIORITIZING MULTIPLE INCIDENTS

Use business impact and likelihood of spread. Assign owners, isolate the highest risk first, and give regular updates to stakeholders. A simple severity matrix keeps everyone aligned.

MEMORY ANALYSIS QUICK

Capture RAM, analyze with a memory framework to find injected code, suspicious handles, and network artifacts, and confirm with EDR timeline and logs. Preserve evidence and document actions.

VULNERABILITY MANAGEMENT AND PENETRATION TESTING

PRIORITIZING SCAN RESULTS

Start with CVSS then adjust by exploit availability, asset criticality, exposure, and compensating controls. Set service level targets such as seven days for critical, fourteen for high, and measure time to remediate.

VULNERABILITY VS EXPLOIT VS PAYLOAD

A vulnerability is the weakness, an exploit is the method that triggers it, and the payload is what executes after exploitation such as a reverse shell or credential dumper.

OWASP TOP TEN THEMES WITH MITIGATIONS

- Broken access control: enforce server-side checks and least privilege
- Cryptographic failures: use modern TLS and never homegrown crypto
- Injection: parameterized queries and input validation
- Insecure design: threat model early and add security controls to the design
- Security misconfiguration: baselines and IaC and continuous scanning
- Vulnerable components: software composition analysis and SBOM
- Identification and authentication failures: strong session management and MFA
- Data integrity failures: signed updates and tamper checks
- Logging and monitoring failures: centralized logs and alerts
- Server-side request forgery: deny by default on outbound and use allow lists

PRIVILEGE ESCALATION APPROACH

Enumerate misconfigurations and weak services and cached credentials then chain small findings to move from user to admin. Always document preconditions scope and impact.

AUTHENTICATED VS UNAUTHENTICATED SCANS

Authenticated give depth and configuration insight while unauthenticated show exposure from an external view. Use both.

SECURITY ARCHITECTURE AND ZERO TRUST

ZERO TRUST PILLARS

Never trust by default. Always verify user device and context. Grant smallest possible access and continuously monitor. Device posture and identity become the perimeter.

SECURE DMZ FOR A WEB APP

Place a reverse proxy or WAF at the edge. Keep web app and database on separate tiers. Allow only required ports between tiers. Terminate TLS at the edge or end to end and rotate secrets.

DEFENSE IN DEPTH

Layer preventive detective and responsive controls so failure of one does not expose the asset. Example is MFA plus EDR plus logging plus network ACLs plus immutable backups.

SEGMENTING HIGH SECURITY WORKLOADS

Use dedicated subnets or VPCs and private endpoints and strict ACLs. Admin comes only from hardened workstations with just in time elevation. No direct internet.

DESIGN REVIEW CHECKLIST

Identify trust boundaries data flows identities and secrets. Validate logging encryption and error handling. Confirm failure modes and test recovery.

• SAST (Static Application Security Testing) reads code without running it

• DAST (Dynamic Application Security Testing) probes a running app from the outside

• IAST (Interactive Application Security Testing) observes from inside during runtime tests

Use more than one because each sees different classes of bugs.

INFRASTRUCTURE AS CODE IMPACT

IaC enforces secure defaults through reusable modules and enables code review on infrastructure. Add policy as code to block risky patterns automatically.

AUTOMATING COMPLIANCE CHECKS

Map controls to machine checks such as CIS benchmarks and cloud config rules. Pull evidence from APIs and generate reports on schedule. Open tickets automatically on drift.

DEVSECOPS AND AUTOMATION

SHIFT LEFT SECURITY

Build security into design and build phases so you catch issues before deployment. It reduces cost and accelerates releases because you avoid rework.

SECURITY IN CI AND CD

Add SAST for code, SCA for dependencies, secret scanning, IaC policy checks, and container image scanning. Block merges on critical findings and require approvals with context.

SAST VS DAST VS IAST

• SAST (Static Application Security Testing) reads code without running it

• DAST (Dynamic Application Security Testing) probes a running app from the outside

• IAST (Interactive Application Security Testing) observes from inside during runtime tests

Use more than one because each sees different classes of bugs.

INFRASTRUCTURE AS CODE IMPACT

IaC enforces secure defaults through reusable modules and enables code review on infrastructure. Add policy as code to block risky patterns automatically.

AUTOMATING COMPLIANCE CHECKS

Map controls to machine checks such as CIS benchmarks and cloud config rules. Pull evidence from APIs and generate reports on schedule. Open tickets automatically on drift.

SECURE SDLC AND THREAT MODELING

SDLC (SOFTWARE DEVELOPMENT LIFE CYCLE) WITH SECURITY ACTIVITIES

- Plan: define security requirements and risk appetite
- Design: build data flow diagrams and threat models and security architecture
- Build: follow secure coding standards and use static analysis and secret scanning
- Test: run DAST and IAST and fuzzing and abuse case testing
- Deploy: harden images and enforce least privilege and sign artifacts
- Maintain: patch, monitor, and collect telemetry for feedback

THREAT MODELING WITH STRIDE

Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege.

STEPS

1. Draw the system with trust boundaries
2. Enumerate assets and entry points
3. Identify threats per STRIDE
4. Assign mitigations and owners
5. Validate in tests

SECURE CODING ESSENTIALS

• Input validation and canonicalization

• Parameterized queries and ORM for database

• Output encoding for HTML and JSON to prevent XSS

• Strong session management with secure cookies and rotation

• Secrets in a manager not in code or environment files

• Structured logging without sensitive data and trace ids for correlation

SUPPLY CHAIN SECURITY

• SBOM (Software Bill of Materials) produced in builds

• Pin dependency versions and verify signatures

• Build in isolated runners and sign artifacts

• Verify in deployment with admission control

GENERAL SOFTWARE DEVELOPMENT FUNDAMENTALS

OOP (OBJECT-ORIENTED PROGRAMMING) PRINCIPLES

Encapsulation hides internals, inheritance reuses behavior, polymorphism changes behavior behind a common interface, abstraction exposes only what is necessary. In interviews give a small example of a Shape interface with concrete classes.

1. Encapsulation
    a. Bundling data and methods into a single unit (object).
2. Abstraction
    a. Shows only essential features while hiding complex implementation details.
3. Inheritance
    a. Allows a class (child/subclass) to inherit properties and methods from another class (parent/superclass).
4. Polymorphism
    a. Means "many forms" — the same method name behaves differently depending on the object that calls it.

API DESIGN

REST uses stateless resources with JSON and clear nouns and proper verbs. Use idempotent operations for safe retries. Return meaningful HTTP status codes and include correlation ids and rate limit headers.

AGILE BASICS

Iterative development with sprints, a prioritized backlog, user stories with acceptance criteria, and regular retrospectives. Definition of done includes tests and security checks.

CI AND CD

Continuous integration merges small changes with automated tests. Continuous delivery automates promotion through environments with approvals. Add security gates in both.

DATA AND RELIABILITY

ACID (Atomicity, Consistency, Isolation, and Durability) transactions for relational systems, eventual consistency for distributed systems, retry with backoff, circuit breakers, and idempotency to handle failures.

	Meaning	Ensures…	Example
Atomicity	All or nothing	No partial updates	Money transfer rolls back if one step fails
Consistency	Valid state before & after	Data integrity and rules enforced	Withdrawal fails if it makes balance negative
Isolation	No interference between transactions	No dirty reads or race conditions	Two users can't buy the same product simultaneously
Durability	Once committed, it's permanent	Data survives crashes	Transaction is still recorded after a power outage

TOP 20 RAPID FIRE INTERVIEW Q AND A

1. **What is Zero Trust**

   Never trust by default, always verify user and device, least privilege on every request, and continuous monitoring.

2. **Hashing vs encryption**

   Hashing is one way for integrity and password storage. Encryption is two way for confidentiality.

3. **Purpose of a POA&M**

   Tracks control gaps with owners milestones and risk so leaders can remediate or accept.

4. **Secure an S3 style bucket fast**

   Block public access at account level, require explicit policies, enable access logs, and scan for exposure.

5. **Least privilege explained**

   Grant only the permissions required to perform a task and nothing more and remove when no longer needed.

6. **IDS vs IPS**

   IDS detects and alerts. IPS sits inline and blocks.

7. **What does a certificate do**

   Binds a public key to an identity and enables encrypted and authenticated sessions.

8. **Defense in depth**

   Multiple layers of preventive detective and responsive controls so single failures do not cause compromise.

9. Symmetric vs asymmetric in TLS

Asymmetric to agree on a session key then symmetric for fast data encryption. **10.**

Lateral movement

Moving from one system to others after initial access often using stolen credentials.

11. SAST vs DAST

SAST reads code without running it. DAST tests a running app from the outside.

13. CIA triad

Confidentiality integrity availability.

14. TLS handshake idea

Negotiate parameters authenticate the server and derive session keys then encrypt the channel.

15. IOC

Indicator of compromise such as a hash domain or IP.

16. Shared responsibility

Provider secures infrastructure and you secure configuration identities and data.

17. Purpose of subnetting

Reduce broadcast domain size and improve security and management by dividing networks.

18. SaaS vs PaaS vs IaaS

SaaS is applications. PaaS is platforms for building. IaaS is raw compute and storage.

19. MAC vs DAC

Mandatory access control enforces central policy. Discretionary access control lets owners set permissions.

20. Risk vs threat

Risk is the potential for loss given a threat and a vulnerability. A threat is something that can cause harm.

CHEAT SHEETS AND QUICK REFERENCE

OSI MODEL

Physical

Data link

Network

Transport

Session

Presentation

Application

COMMON PORTS

22 SSH

25 SMTP

53 DNS

80 HTTP

110 POP3

143 IMAP

389 LDAP

443 HTTPS

445 SMB

1433 Microsoft SQL

3306 MySQL

3389 RDP

SUBNET QUICK CHART

Slash 24 has 254 usable

Slash 25 has 126 usable

Slash 26 has 62 usable

Slash 27 has 30 usable

Slash 28 has 14 usable

Slash 29 has 6 usable

Slash 30 has 2 usable

Usable hosts formula is two to the power of host bits minus two

WINDOWS EVENT IDS TO MEMORIZE

4624 logon success

4625 logon failure

4672 special privileges assigned

4688 process creation

4697 service installed

4720 account created

4732 member added to local group

4776 NTLM authentication

7045 service creation in system log

LINUX QUICK COMMANDS

last login history

journalctl -xe recent errors

ss -tupn sockets

lsof -i network file descriptors

auditctl -l audit rules

FAST SUBNET PRACTICE WITH ANSWERS

• How many hosts in 172.20.0.0 slash 19

32 minus 19 equals 13 so 8192 total and 8190 usable

• First and last usable of 192.168.50.64 slash 27

Usable .65 through .94

EXTRA NETWORKING STUDY BLOCK

NAT TYPES

• Static one to one mapping

• Dynamic pool mapping

• Port address translation many to one using ports

ACL TIPS

• Place standard ACLs near destination and extended ACLs near source

• Deny statements should be followed by explicit permits to avoid accidental lockouts

• Log matches to see impact

DNS SECURITY REMINDERS

- Validate DNSSEC to prevent cache poisoning
- Do not run open resolvers
- Log and hunt on rare domains and newly seen domains

CLOSING TIP

Practice giving every answer in two or three clean sentences first, then add one deeper note that shows practical experience. That structure wins interviews: definition, why it matters, and how you apply it.