DNS Troubleshooting & Security Guide

Interview Preparation for Networking, Cloud & DevOps

Last Updated: January 18, 2026

1. Core Troubleshooting Tools: nslookup vs. ping vs. tracert

In network troubleshooting, distinguishing between DNS resolution issues and network connectivity issues is critical. These three tools serve distinct purposes in the diagnostic workflow.

Comparison Overview

Tool	Primary Purpose	Question It Answers	Key Limitations
nslookup / dig	DNS Diagnostics	"What IP belongs to this domain name?"	Does NOT check if the server is online or reachable; only checks the phonebook entry.
ping	Connectivity Check	"Is the server alive and reachable?"	Relies on ICMP, which is often blocked by firewalls;

			doesn't show the path taken.
tracert / traceroute	Path Analysis	"Where is the connection breaking along the route?"	Slow execution; routers often de-prioritize or block ICMP/UDP trace packets.

Real-World Analogy: The Pizza Delivery

- nslookup: Checking the phone book to find the pizza shop's address. (You haven't left your house yet).
- ping: Driving to the pizza shop and knocking on the door to see if they are open.
- tracert: Driving to the shop and noting every intersection and traffic light you pass to see where the traffic jam is.

Detailed Breakdown & Syntax

A. nslookup (Name Server Lookup)

Used to query DNS servers directly. It bypasses the local OS cache in many implementations to query the configured DNS server.

- Windows/Linux/macOS: `nslookup example.com`
- Linux/macOS Alternative (More powerful): `dig example.com`

```
      C:\> nslookup google.com Server: dns.google Address: 8.8.8.8
Non-authoritative answer: Name: google.com Addresses:
      142.250.190.46 2607:f8b0:4009:80b::200e
```

B. ping (Packet Internet Groper)

Sends ICMP Echo Request packets to test reachability and measure round-trip time (latency).

- Windows: `ping google.com` (Sends 4 packets by default)
- Linux/macOS: `ping google.com` (Runs continuously until Ctrl+C)

```
      $ ping -c 4 google.com PING google.com (142.250.190.46): 56
data bytes 64 bytes from 142.250.190.46: icmp_seq=0
      ttl=117 time=14.2 ms 64 bytes from 142.250.190.46: icmp_seq=1
ttl=117 time=13.8 ms ... --- google.com ping
      statistics --- 4 packets transmitted, 4 packets received, 0.0%
packet loss
```

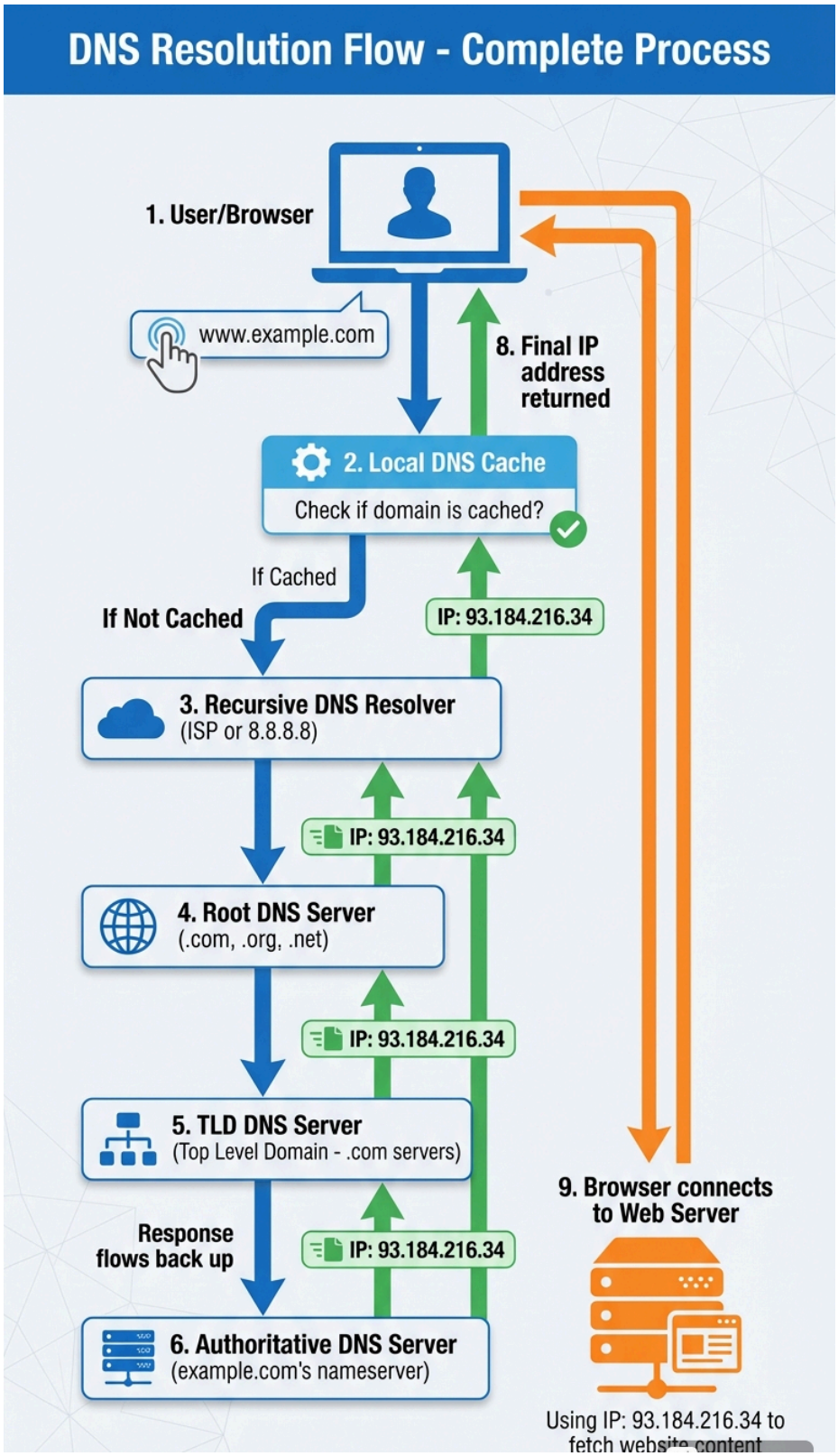
C. tracert (Windows) / traceroute (Linux/macOS)

Maps the network hops between source and destination by manipulating packet TTL (Time To Live). Useful for identifying which router is dropping packets.

- Windows: `tracert google.com` (Uses ICMP)
- Linux/macOS: `traceroute google.com` (Default uses UDP; often requires `-I` for ICMP)

```
      C:\> tracert google.com Tracing route to google.com
[142.250.190.46] over a maximum of 30 hops: 1 <1 ms <1 ms <1
      ms 192.168.1.1 (Local Router) 2 8 ms 9 ms 8 ms 10.20.0.1 (ISP
Gateway) 3 15 ms 14 ms 15 ms 142.250.190.46
      (Destination) Trace complete.
```

DNS Resolution Flow Diagram



2. DNS Security Concerns

DNS was designed in the 1980s without built-in security. Consequently, it is vulnerable to various attacks aimed at redirection, denial of service, or information leakage.

A. DNS Spoofing / Cache Poisoning

How it works: An attacker inserts corrupt DNS data into the cache of a recursive DNS server. When legitimate users query that server, they receive the attacker's fake IP address and are redirected to a malicious site (e.g., a fake banking login).

- Indicators: Users redirected to wrong sites; SSL certificate errors (if the attacker doesn't have a valid cert).
- Impact: Phishing, credential theft, malware distribution.
- Prevention/Mitigation:
  - DNSSEC (DNS Security Extensions): Cryptographically signs DNS records to validate authenticity.
  - Randomize Source Ports: Makes it harder for attackers to guess the transaction ID.
  - Flush Caches: Immediate remediation step during an incident.

B. DNS DDoS / Amplification Attacks

How it works: Attackers spoof the victim's IP address and send small DNS queries (like "ANY") to open DNS resolvers. The resolvers reply with large responses to the victim, overwhelming their bandwidth.

- Indicators: Massive spike in inbound traffic (UDP port 53); high load on DNS servers; network saturation.
- Impact: Service unavailability; collateral damage to upstream ISPs.
- Prevention/Mitigation:
  - Response Rate Limiting (RRL): Configures the server to slow down responses to specific request patterns.
  - Disable Open Recursion: Configure DNS servers to only accept recursive queries from trusted internal networks.
  - Access Control Lists (ACLs): Restrict who can query the server.

C. DNS Oversharing (Zone Transfers & Leakage)

How it works: Misconfigured DNS servers allow unauthorized users to request a full copy of the DNS zone (AXFR request). This reveals the entire internal network map, including subdomains, internal IP schemes, and server names.

- Indicators: `dig axfr @ns1.target.com` succeeds from an external IP.
- Impact: Reconnaissance data for attackers; reveals potential high-value targets (e.g., `dev-db.corp.local`).
- Prevention/Mitigation:
  - Restrict Zone Transfers: Allow transfers only to known secondary DNS server IPs.
  - Split-Horizon DNS: Maintain separate DNS views for internal and external users.
  - Minimal Responses: Configure servers to return minimal information ("refused") for unauthorized queries.
  - TSIG (Transaction SIGnature): Require authentication for zone transfers.

Emerging Mitigation: DoH and DoT

To prevent eavesdropping and manipulation, modern clients use:

- DNS over HTTPS (DoH): Encrypts DNS traffic inside HTTPS (Port 443). Hard to block/monitor.
- DNS over TLS (DoT): Encrypts DNS traffic over TLS (Port 853). Dedicated secure channel.

3. Answering Behavioral Questions: The STAR Method

When answering "Tell me about a time..." questions, structure your response using STAR: Situation, Task, Action, Result.

Example: DNS Incident Response

Question: "Tell me about a time you troubleshot a critical network issue."

Situation: "In my previous role as a DevOps Engineer, we experienced a sudden outage where internal employees could not access our CRM tool, although the application server itself was running."

Task: "My task was to identify the root cause of the connectivity failure and restore access for the 200 affected sales staff immediately."

Action: "I started by verifying the server status, which was green. I then used `nslookup` and noticed it was failing to resolve the internal domain name. I checked the DNS server logs and found the service had hung due to a memory leak. I immediately restarted the DNS service to restore temporary access, then scheduled a patch update for the maintenance window to fix the memory leak permanently."

Result: "The service was restored within 10 minutes. The patch applied later that night prevented any recurrence, and I implemented a new monitoring alert for DNS service memory usage to catch this early in the future."

STAR Template for Interview Notes

- S: Context (Who, What, Where, When).
- T: The specific challenge or goal.
- A: What *YOU* did (Focus on "I", not "We"). Detailed technical steps.
- R: The outcome (Quantify if possible: % uptime, $ saved, time reduced).

4. Interview Questions Bank

Part A: Scenario-Based (Technical)

1. "Users report they can't access a website, but they can ping the IP address. What is the problem?"

Expected Answer:

- Identify this as a DNS resolution failure.
- Explain that pinging by IP confirms network connectivity (Layer 3) is working.

- Troubleshooting steps: Check `nslookup`, flush local DNS cache (`ipconfig /flushdns`), check if the configured DNS server is reachable.

2. "We are migrating our website to a new hosting provider. How do you ensure zero downtime during the DNS switch?"

Expected Answer:

- TTL Strategy: Lower the TTL (Time to Live) on the DNS records to 300 seconds (5 mins) a few days before migration.
- Propagation: Wait for the old TTL to expire globally.
- Switch: Update the A record to the new IP.
- Post-Switch: Once verified, raise the TTL back to normal (e.g., 24 hours).

3. "You see a huge spike in UDP traffic on port 53 coming from random external IPs. What is happening?"

Expected Answer:

- Identify this as a likely DNS Amplification/DDoS attack or the server is being used as an open resolver.
- Immediate Action: Enable Response Rate Limiting (RRL).
- Mitigation: verify "recursion" is disabled for external IPs in the configuration (e.g., `allow-recursion { local_subnets; };` in BIND).

4. "A developer created a new subdomain dev.example.com, but external users get an NXDOMAIN error. It works inside the office. Why?"

Expected Answer:

- Suspect Split-Horizon DNS.
- The internal DNS view has the record, but the external (public) DNS view has not been updated.
- Solution: Add the A record to the public-facing DNS zone file.

5. "How does DNSSEC protect against cache poisoning?"

Expected Answer:

- Explain the Chain of Trust.
- DNSSEC adds digital signatures (RRSIG) to records.
- Resolvers verify the signature using the public key (DNSKEY).
- If the signature doesn't match the data (modified by an attacker), the resolver rejects the answer.

Part B: Behavioral

1. "Describe a time you had to explain a complex technical issue to a non-technical stakeholder."

Key Elements: Use the "Address Book" analogy for DNS. Focus on business impact (downtime/cost) rather than technical jargon (A records/CNAMEs).

2. "Tell me about a time you made a mistake on a production system."

Key Elements: Own the mistake immediately. Focus on the recovery process and the systemic fix you implemented to prevent it from happening again (e.g., "I deleted a DNS record by accident... I restored it from backup... I then implemented a 'peer review' requirement for all DNS changes").

3. "Have you ever disagreed with a senior engineer's approach? How did you handle it?"

Key Elements: Focus on data and testing. "I set up a test environment to demonstrate that my proposed TTL setting would reduce load better than their suggestion."

4. "Describe a situation where you had to troubleshoot a problem with limited information."

Key Elements: Systematic isolation. "I didn't know the network topology, so I used `traceroute` to map it out myself..."

5. "How do you stay updated with security threats like DNS tunneling?"

Key Elements: Mention specific sources (CVE feeds, Hacker News, security blogs like Krebs on Security). Mention practicing in home labs.

Part C: Rapid Fire (Concept Check)

- What is an A Record? Maps a hostname to an IPv4 address.
- What is a CNAME? An alias pointing one domain name to another domain name.
- What is a PTR Record? Reverse DNS; maps an IP to a hostname.
- Default DNS Port? UDP 53 for queries, TCP 53 for zone transfers/large responses.
- What does TTL stand for? Time To Live – how long a record stays in cache.