Support Triage Task + Scoring Rubric

Portfolio demonstration by Yohanan Moraes | Customer support, infrastructure and AI evaluation

FICTIONAL PORTFOLIO EXERCISE - NOT CLIENT WORK

1. Task objective

Assess whether a support specialist can turn an ambiguous certificate complaint into a safe, evidence-based routing decision. The answer must identify the likely fault domain, propose reproducible checks, recommend a low-risk resolution and communicate clearly to the customer.

2. Fictional customer ticket

Customer	Northstar Analytics (fictional)
Environment	SaaS application behind Cloudflare; Nginx origin; managed TLS certificate
Ticket	"Some users see a certificate warning after we changed www to app. It works in our office but often fails on phones."
Impact	Intermittent access failure; no confirmed data loss; mobile users appear more affected

3. Evidence available to the specialist

- DNS: app.northstar.example has A 203.0.113.24; www is a CNAME to app.
- A stale AAAA record still points to 2001:db8:dead:beef::24, the former origin.
- The managed certificate covers app and www and expires in 65 days.
- curl -4 returns HTTP 200 with the expected certificate; curl -6 reaches a different certificate.
- Reports are concentrated on mobile networks where IPv6 is preferred.
- The customer can edit DNS but has not approved a change yet.

4. Candidate instructions

- Classify impact and urgency using plain language; do not invent a proprietary severity code.
- State the leading hypothesis and identify the likely fault domain.
- List the minimum verification steps and commands needed to confirm or reject the hypothesis.
- Recommend a safe resolution sequence, including approval, backup and post-change validation.
- Write a concise customer-facing response and define escalation triggers.

5. Reference resolution path

The strongest hypothesis is a stale IPv6 DNS path sending mobile clients to the former origin, where the wrong certificate is presented. The current certificate itself is not expired and already contains both hostnames. Confirm with dig A/AAAA, curl -4/-6 -Iv and openssl s_client using SNI for both hostnames. After customer approval and a saved DNS snapshot, update or remove the stale AAAA record, wait for TTL propagation and repeat IPv4/IPv6 checks. Do not disable TLS, ignore the warning or switch to an insecure SSL mode.

Scoring Rubric

Passing score: 80/100, provided no critical-failure rule is triggered. Scores are based on observable evidence, not writing style alone.

Criterion	Weight	Full-credit evidence
Evidence extraction	15	Connects mobile impact, IPv6 preference, stale AAAA and certificate mismatch without treating correlation as proof.
Hypothesis and fault domain	20	Identifies stale IPv6 routing to the former origin as the leading hypothesis and distinguishes DNS/origin configuration from certificate expiry.
Verification plan	20	Uses A/AAAA lookup, IPv4/IPv6 curl, SNI-aware TLS inspection and tests both hostnames before recommending change.
Safe resolution	20	Requires approval and DNS snapshot, updates or removes stale AAAA, respects TTL and validates both network paths after change.
Customer communication	15	Explains partial impact, likely cause, verification and next action without blame, jargon overload or false certainty.
Escalation and documentation	10	Escalates on inconsistent authoritative DNS, unmanaged origin ownership, persistent mismatch after propagation or evidence of broader compromise.

Critical-failure rules

- Recommends disabling TLS, bypassing browser warnings or using an insecure SSL mode.
- Makes a destructive DNS change without approval, rollback evidence or post-change validation.
- Claims that certificate renewal is the primary fix despite correct SANs and remaining validity.
- Ignores the IPv6 path even though the evidence isolates the mismatch to that route.

Any critical failure caps the score at 49 because it creates security or availability risk even if other sections are strong.

Calibration anchors

90-100	Complete, safe and reproducible. Separates hypothesis from proof and produces a customer-ready response.
80-89	Correct route and safe fix with one minor omission, such as a less explicit rollback or escalation trigger.
60-79	Finds the likely cause but verification, safety controls or communication are incomplete.
0-59	Misses the IPv6 evidence, proposes an unsafe action or cannot define an objective resolution path.

Design note: all domains and IP addresses use reserved examples. No credentials, customer data or real production systems are represented.