TROUBLESHOOTING ESSENTIALS · COURSE TOOLKIT

Final Revision Guide

> **Toolkit 9 of 10** · Final Revision Guide · Summarises Parts I–IV of Dr. Tahseen Al Doori's *Troubleshooting Essentials*, University Edition (2026). Lists are the author's; the exam traps and layout are the course's.

How to use this guide

There is one page for each part of the course. For each page: read the key lists aloud without looking, then check yourself against the page; read the **common exam traps**, which are the mistakes learners make most often in scenario questions; then answer the self-test prompts at the bottom. Revisit any module where you hesitate. Use this guide in the week before the Final Assessment, alongside the One-Page Checklist (Toolkit 1).

Page 1 — Part I: Foundations (Modules 1–3)

Key definitions

- **Troubleshooting:** the systematic process of identifying, diagnosing and resolving problems so that a system returns to normal operation.
- **Repair:** correcting a known fault. **Maintenance:** planned work that keeps a system healthy before it fails.

Key lists

LIST	ITEMS
Four benefits of a structured method	Speed · Safety · Repeatability · Knowledge
Six problem categories	Hardware · Network · Software · Account and access · User and process · Environmental
Seven principles	Stay calm · Be curious, not certain · Start simple · Change one thing at a time · Observe before acting · Protect what matters · Write it down
Common mistakes	Jumping to a fix · Ignoring error messages · Changing many things at once · Assuming "it can't be that" · Not asking what changed · Working without notes
Four biases	Confirmation · Anchoring · Availability · Sunk-cost
Seven steps	1 Identify the problem · 2 Establish a theory of probable cause · 3 Test the theory to determine the cause · 4 Establish a plan of action · 5 Implement the solution or escalate · 6 Verify full system functionality · 7 Document findings, actions and outcomes

Identify → Theory → Test → Plan → Implement → Verify → Document

Common exam traps

- Confusing **anchoring** (fixing on the first information, such as the user's own diagnosis) with **confirmation bias** (seeing only evidence that supports your theory) and **availability bias** (assuming the cause of the last similar problem).
- Forgetting the **loop**: a rejected theory sends you back to **Step 2**, not forward to Step 4.
- Placing the **rollback plan** in Step 5. It is prepared in **Step 4**, before anything changes.
- Closing a problem before the **user confirms** it works (Step 6).
- Treating maintenance as troubleshooting: if nothing has failed, it is maintenance.

Self-test: State the output of each of the seven steps. Name the principle broken when three changes are made at once.

Page 2 — Part II: Diagnostic Techniques (Modules 4–7)

Key lists

LIST	ITEMS
5W1H	What · When · Where · Who · **Which** (which changes happened just before) · How
Evidence	Exact error messages · Physical symptoms · Logs and history · Scope · Recent changes
Five quick wins, in order	1 Power · 2 Connections · 3 Restart · 4 Settings and input · 5 Updates, storage and resources
What a restart does	Clears temporary memory · Ends stuck processes · Reloads drivers and configuration · Re-establishes network connections
Six isolation techniques	Half-split · Substitution · Comparison · Following the path (bottom-up, top-down, follow the flow) · Remove and restore · Rollback
Five-step connectivity sequence	ping 127.0.0.1 · ipconfig · ping default gateway · ping 8.8.8.8 · ping a name

Choosing a technique: long chain → half-split · spare parts → substitution · identical working system → comparison · began after a known change → rollback · many add-ons → remove and restore · no obvious start → bottom-up · only one application affected → top-down.

Problem statement template (the book's): "Since [when], [who] cannot [what] on [where]. It happens [always / intermittently] when [how]. The most recent change was [which]. The error shown is “[exact message]”."

Common exam traps

- Writing **Why** instead of **Which** in 5W1H. In this course, the fifth W is Which.
- Asking closed questions first. **Open questions come first**.
- Putting the quick wins in the wrong order, especially restarting before checking power.
- Treating a repeated restart as a fix. **If a quick win has to be repeated, it is a workaround.**
- Half-split arithmetic: 8 components need at most **3** tests, 16 need **4**, 1,000 need **10**.
- Reading 169.254.x.x as a DNS fault. It means **no response from a DHCP server**.
- Forgetting that the **first failing step** of the connectivity sequence shows where the fault lies.

- Network power-cycle order: **modem, wait 60 seconds, router, then the end device**.

Self-test: A user can ping 8.8.8.8 but not open websites by name: what is the fault? Where are system logs on Windows, macOS and Linux?

Page 3 — Part III: Applying the Method (Modules 8–11)

Key points by area

AREA	REMEMBER
No power	Check the supply chain from socket to device; remove accessories; laptops: hold power button 15–30 seconds to discharge; observe fans, lights, beeps
No boot	Read the codes and messages. "No boot device found" → firmware (BIOS/UEFI) settings and drive connection. Restart loop → safe mode or recovery; roll back update. Error screen → record stop code
Slow or freezing	Restart; keep 10–15% of the drive free; check processes; disable startup items; updates and malware scan; heat; consider SSD
Failing storage	Clicking, slow access, corrupt files, disk errors → **back up immediately and stop unnecessary use**
Failing memory	Random crashes, error screens, corrupted files → memory diagnostic; test one module at a time
Networks	First question: **one device or all?** Then work through the layers. Gateway reachable but no internet → router, modem or provider. By IP works, by name fails → DNS
Applications	Eight steps from recording the error to searching the vendor's knowledge base; private window and second browser isolate web faults
Updates and drivers	Fault right after an update → roll back (Roll Back Driver, System Restore), report to vendor, pause that update; never leave a system permanently unpatched
Accounts	Caps Lock and layout · lockout · expiry · saved old credentials or wrong clock on one device · Access denied → permissions. **Never ask for a password**
Malware	Ransom message → disconnect from the network, do not pay or interact, report to IT security
Peripherals	Separate the device from the computer: printer test page, headset on another device. The half that fails holds the fault

Common exam traps

- Running a disk repair on a failing drive before backing up.
- Blaming the provider when only **one** device is affected.
- Forgetting that a printer that prints its own test page has a fault in the **computer or network**.
- Doing a factory reset on a phone before backing up; it is the **last resort**.
- Unexpected characters from a keyboard: check the **language and layout** setting before suspecting hardware.

Self-test: List four checks for a projector showing nothing from a laptop. Give three reasons a correct password might be rejected.

Page 4 — Part IV: Resolution and Professional Practice (Modules 12–14)

Key lists

LIST	ITEMS
Four terms	Symptom (what is observed) · Workaround (temporary way to keep working) · Fix (corrects the immediate fault) · Root cause (underlying reason)
Root cause tools	5 Whys for a single chain of cause · Fishbone diagram when many factors may contribute (people, process, technology, network, environment, measurement)
Preventive measures	Scheduled, tested updates · Regular, verified backups · Monitoring and alerts · Standard configurations · Change management · Labelled cables and documented networks · User training and clear guides · Clean, cool, protected equipment
Escalation triggers	Safety · Data · Security · Authority or access · Warranty or contract · Theories exhausted or time limit passed · Many users or critical services
Support tiers	0 Self-help · 1 Help desk · 2 Technical support · 3 Specialists · 4 Vendor / external
Six-part handover	Problem statement · Exact errors and evidence · When it started and what changed · Every action and result · Urgency and users affected · Contact details and availability
Communicating with users	Listen fully and acknowledge impact · Plain language, no jargon or blame · Realistic expectations · Keep users informed · Confirm the fix before closing
Four case studies	Office without internet (one device or all; valid IP and router ping but no 8.8.8.8 → outside the office) · Slow laptop (resource monitoring; storage full and disk at 100%) · Intermittent Wi-Fi (occurrence log; microwave on 2.4 GHz) · Late deliveries (analysis by courier and product; method works beyond IT)

Common exam traps

- Calling a workaround a fix, or a fix a root-cause fix. Ask: **will it come back?**
- Ending the 5 Whys at a person ("user error") instead of a correctable process.
- Using the 5 Whys where several factors contribute (fishbone is better).
- Getting the tiers in the wrong order, or forgetting **Tier 0** (self-help) and **Tier 4** (vendor or external, including the internet provider).
- Omitting **every action and its result** from a handover: the next person then starts again.
- Continuing to troubleshoot when a safety trigger appears (swollen battery, burning smell). **Stop and escalate.**

Self-test: Name the six parts of a handover in order. Which single test in Case Study 1 proved the fault was outside the office network?

Sources

- Dr. Tahseen Al Doori — *Troubleshooting Essentials*, University Edition (2026), Chapters 1–14