TROUBLESHOOTING ESSENTIALS · COURSE TOOLKIT

Course Glossary

Toolkit 10 of 10 · Course Glossary · Terms marked † are from the Glossary of Dr. Tahseen Al Doori's *Troubleshooting Essentials*, University Edition (2026), with definitions adapted; other terms are added by the course from the book's chapters (module shown in brackets).

How to use this glossary

Terms are in alphabetical order (numbers sort as words: "5 Whys" under F, "5W1H" under F). When you meet an unfamiliar term in a lesson, look it up here, then return to the module shown for the full explanation. For revision, cover the definitions and try to explain each term in your own words.

TERM	DEFINITION
Activity Monitor	The macOS tool that shows running processes and their use of CPU, memory, energy, disk and network. (Module 7)
Anchoring	A cognitive bias: fixing on the first piece of information received, such as a user's own diagnosis, and failing to look beyond it. (Module 2)
Anti-static wrist strap	A strap that protects components from electrostatic discharge while equipment is open. (Modules 7, 8)
Availability bias	A cognitive bias: assuming the cause is whatever caused the last similar problem. (Module 2)
Baseline †	A record of how a system looks and performs when it is working normally, used to make abnormal behaviour visible. (Module 4)
Beep code	A pattern of beeps produced by a computer's firmware at start-up to report a hardware fault; look it up in the manufacturer's documentation. (Module 8)
Bottom-up approach †	Troubleshooting that starts at the physical level (power, cables, hardware) and works upwards to software and settings. (Module 6)
Change management	A controlled process for planning, approving and recording changes, which prevents faults introduced by unplanned changes. (Module 12)
Comparison	An isolation technique: placing a faulty system beside an identical working one and comparing settings, versions, cables and behaviour; the difference is usually the cause. (Module 6)
Confirmation bias	A cognitive bias: noticing only the evidence that supports the first theory and ignoring evidence against it. (Module 2)
Default gateway	The router a device sends traffic to when the destination is outside its local network. Being able to ping it is step 3 of the connectivity sequence. (Modules 7, 9)
Device Manager	The Windows tool that lists hardware devices and driver status, shows warning icons for faulty devices and offers Roll Back Driver. (Modules 7, 10)
DHCP †	Dynamic Host Configuration Protocol: the service that automatically assigns IP addresses and related settings to devices. (Modules 7, 9)
DNS †	Domain Name System: the service that translates names such as example.com into IP addresses. (Modules 7, 9)
Downtime	A period in which a system is unavailable; it costs individuals time and organisations sales, productivity, deadlines and reputation. (Module 1)
Escalation †	Passing a problem to someone with more skill, access or authority. (Module 13)
Escalation trigger	A condition that means stop and escalate: safety, data, security, authority or access, warranty or contract, theories exhausted or time limit passed, many users or critical services affected. (Module 13)
Event log †	A system record of errors, warnings and significant events, with times and codes. (Module 7)
Event Viewer	The Windows tool for reading event logs, grouped under Windows Logs (Application, System and Security). (Module 7)
Fishbone diagram †	A cause-and-effect diagram (also called an Ishikawa diagram) that groups possible causes of a problem into categories such as people,

TERM	DEFINITION
	process, technology, network, environment and measurement. (Module 12)
Five quick-win checks	The five basic checks performed first, in order: power, connections, restart, settings and input, and updates, storage and resources. (Module 5)
5 Whys †	A root cause technique that asks why a problem occurred, usually about five times, until it reaches a cause that can be corrected. (Module 12)
5W1H †	What, When, Where, Who, Which and How: the questions that define a problem. *Which* asks which changes happened just before the fault. (Module 4)
Follow the flow	A path-following approach that traces data or a signal from its source to its destination, checking each stage. (Module 6)
Half-split †	Testing the midpoint of a system to find which half contains the fault, then repeating on that half; each test removes half the possibilities. (Module 6)
Handover	The information passed to the next person when a problem is escalated, in six parts: problem statement; exact errors and evidence; when it started and what changed; every action and result; urgency and users affected; contact details and availability. (Module 13)
Intermittent fault †	A problem that comes and goes; often the hardest kind to diagnose because it disappears when examined. (Module 4)
IP address	The numerical address that identifies a device on a network. A valid address, subnet mask, gateway and DNS servers are checked with ipconfig or its equivalents. (Modules 7, 9)
Knowledge base	A collection of recorded problems and solutions; consistent documentation of incidents builds one over time. (Module 13)
Known-good †	A component or system confirmed to work, used for comparison or substitution. (Module 6)
Link-local address (169.254.x.x)	An IPv4 address in the 169.254/16 range that a device configures for itself when no stable, routable address is available (defined in RFC 3927; beyond the book). In troubleshooting, an address beginning 169.254 means the device received no response from a DHCP server. (Modules 7, 9)
Loopback address (127.0.0.1)	The address a device uses to talk to itself; pinging it tests whether the TCP/IP stack is working locally (step 1 of the connectivity sequence). (Module 7)
Maintenance	Planned work that keeps a system healthy before it fails, such as scheduled updates, cleaning and backups. (Module 1)
Multimeter	A hardware tool for measuring voltage, continuity and resistance in power supplies and cables. (Module 7)
Occurrence log	A record of each occurrence of an intermittent fault with date, time, activity and conditions, kept until a pattern appears. (Module 4)
OSI model †	A seven-layer model of network communication, used as a troubleshooting framework because each layer depends on those beneath it. (Module 9)
Plan of action	The output of Step 4: what will be changed, what could go wrong, how the change will be undone, and any approval, backup and recorded settings needed. (Module 3)

TERM	DEFINITION
Power-cycle †	Turning a device fully off, waiting, and turning it back on. For networks: modem, wait 60 seconds, router, then the end device. (Module 5)
Problem statement †	A specific, factual and testable description of a problem, used to guide diagnosis. (Module 4)
Remove and restore	An isolation technique: reducing a system to its minimum, then restoring items one at a time until the fault returns; the last item restored is the cause. (Module 6)
Repair	Correcting or replacing a component once the fault is known. (Module 1)
Reproduce †	To make a problem happen on purpose so that it can be tested. (Module 4)
Rollback †	Undoing a change to return to the previous working state; also an isolation technique when a problem began after a known change. (Modules 6, 10)
Root cause †	The underlying reason a problem occurs, rather than its symptom. (Module 12)
Safe mode †	A start-up mode that loads only essential drivers and software, used for isolation. (Modules 6, 7)
Seven principles	The author's principles of effective troubleshooting: stay calm; be curious, not certain; start simple; change one thing at a time; observe before acting; protect what matters; write it down. (Module 2)
Seven-step methodology	The author's method used throughout the course: identify the problem; establish a theory of probable cause; test the theory to determine the cause; establish a plan of action; implement the solution or escalate; verify full system functionality; document findings, actions and outcomes. (Module 3)
S.M.A.R.T. †	Self-Monitoring, Analysis and Reporting Technology: the health reporting built into storage drives. (Module 8)
Stop code	The code shown on a blue or black error screen; record it and check recent driver changes. (Module 8)
Substitution †	Replacing a suspected part with a known-good part to test it; if the problem disappears, the removed part was at fault. (Module 6)
Sunk-cost thinking	A cognitive bias: continuing with a failing approach because much time has already been invested in it. (Module 2)
Symptom †	What can be seen or heard going wrong. (Module 12)
Task Manager	The Windows tool (Ctrl+Shift+Esc) that shows running applications, CPU, memory, disk and network use, and startup programs. (Module 7)
Tiered support model	The organisation of support into tiers: Tier 0 self-help, Tier 1 help desk, Tier 2 technical support, Tier 3 specialists, Tier 4 vendor or external. (Module 13)
Top-down approach †	Troubleshooting that starts at the application the user sees and works downwards. (Module 6)
Troubleshooting	The systematic process of identifying, diagnosing and resolving problems in a system so that it returns to normal operation. (Module 1)

TERM	DEFINITION
UPS (uninterruptible power supply)	A battery unit that keeps equipment running through short power cuts; used in Case Study 1 to protect the modem and router. (Module 14)
Verification	Step 6: confirming that the original problem is resolved and nothing else is broken, including the user's confirmation. (Module 3)
Workaround †	A temporary way to keep working while the real fix is found. A quick win that has to be repeated is a workaround, not a fix. (Modules 5, 12)

Sources

- Dr. Tahseen Al Doori — *Troubleshooting Essentials*, University Edition (2026), Glossary and Chapters 1–14
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses — RFC Editor (link-local address)