Network Troubleshooting

CompTIA Network+ certification exam, N10-009

24% of the exam · 5 exam objectives · N10-009

Domain 5 is the largest part of Network+: troubleshooting. It starts with CompTIA's seven-step methodology, which is tested in its exact order, then applies it to cabling and physical interfaces (cable types, signal degradation, interface counters, port status, PoE and transceivers), network services (spanning tree, VLANs, ACLs, routing, DHCP and addressing), performance (congestion, bottlenecks, latency, jitter, packet loss and wireless problems), and the software tools, hardware tools and device commands used to find each fault. Questions describe symptoms; the skill is to read them, name the cause and pick the right tool.

You should be able to: A user reports that a printer cannot be reached since this morning. List the seven steps of the troubleshooting methodology in order, and name the step in which you would ask the user whether anything changed overnight.

Every exam objective: the key point and the trap

5.1 Explain the troubleshooting methodology.

The methodology has seven steps in a fixed order: identify the problem; establish a theory of probable cause; test the theory to determine the cause; establish a plan of action to resolve the problem and identify potential effects; implement the solution or escalate as necessary; verify full system functionality and implement preventive measures if applicable; document findings, actions, outcomes and lessons learned throughout the process.

Trap: Putting the plan of action before testing the theory, or treating verification as the last step. The plan follows a confirmed theory, and documentation runs throughout the process and is completed at the end.

5.2 Given a scenario, troubleshoot common cabling and physical interface issues.

Incorrect cable: single-mode and multimode fiber are not interchangeable; copper category (Category 5, 6, 7, 8) sets the speeds a run supports; STP resists interference where UTP may not.

Trap: Assuming a down port is always a cable fault. Read the port status first: administratively down and error disabled are switch states, and a cable change alone will not bring them up.

5.3 Given a scenario, troubleshoot common issues with network services.

Spanning tree (STP in 5.3, not shielded twisted pair) problems: a network loop (spanning tree off or misconfigured) causes a broadcast storm; an unintended root bridge (lowest bridge ID wins) bends traffic paths; port roles (root, designated) and states (blocking, listening, learning, forwarding) show how STP converged.

Trap: Blaming DHCP for every addressing fault. APIPA points to DHCP; a wrong mask, gateway or duplicate address usually comes from a static entry or a wrong DHCP scope setting.

5.4 Given a scenario, troubleshoot common performance issues.

Congestion or contention: many devices compete for one link or medium, so queues fill and packets drop at busy times.

Trap: Treating bandwidth and throughput as the same. A 1 Gbps link can deliver far less when congested, bottlenecked or losing packets.

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

Protocol analyzers and tcpdump capture and decode packets; a tap copies a link's traffic passively for them.

Trap: Using a cable tester to find where a cable runs (that is the toner), or a copper tester on fiber (that is the visual fault locator).

Key terms

CRC: Cyclic Redundancy Check

PoE: Power over Ethernet

STP: Shielded Twisted Pair

UTP: Unshielded Twisted Pair

TX: Transmitter

RX: Receiver

VLAN: Virtual Local Area Network

ACL: Access Control List

APIPA: Automatic Private Internet Protocol Addressing

LLDP: Link Layer Discovery Protocol

ExamDragon, examdragon.com/netplus. Independent exam preparation, written in our own words to the N10-009 exam objectives. CompTIA and Network+ are trademarks of CompTIA, Inc.