Comp Tia A+ (220-1101) Day 7 Notes

CompTIA Troubleshooting Methodology - Section 5.1

Troubleshooting Steps
("I Eat Tacos, Even Visit Dumpsters")

1. **Identify the problem**
    - Gather information from the user, identify user changes, and, if applicable, perform backups before making changes.
    - Inquire regarding environmental or infrastructure changes.
2. **Establish a theory of probable cause (question the obvious)**
    - If necessary, conduct external or internal research based on symptoms.
3. **Test the theory to determine the cause**
    - Once the theory is confirmed, determine the next steps to resolve the problem.
    - If the theory is not confirmed, re-establish a new theory or escalate.
4. **Establish a plan of action to resolve the problem and implement the solution**
    - Refer to the vendor's instructions for guidance.
5. **Verify full system functionality and, if applicable, implement preventive measures**
6. **Document the findings, actions, and outcomes**

Identify the Problem

Gather data from multiple sources:

- User reports
- Logs and alerts
- Changes made by the user
- Changes made by IT

If necessary and reasonable, perform backups before making changes to a system.

Establish Theory

What is the most likely cause?

- Prioritize the simplest and easiest theories.
- Conduct research as needed:
    - Internal research (knowledge bases, ticketing system)
    - External research (Google, vendor documentation)
        - Use error codes; copy and paste them directly into Google.

Test Theory

- Test one thing at a time, methodically. Multiple changes may prevent identifying the actual fix if a single change would have been sufficient.

Establish a Plan of Action

- Consider:
    - Impact of solutions. Does it require downtime? Does it interfere with a service contract?
    - The importance of the issue.
    - The risk to data.

Verify Full System Functionality

- Did the solution cause any other issues?
- Are there changes that could prevent the issues in the future?

Document

- Share documentation across IT.
- Helps track changes made in case they cause secondary issues.
- Consider recording:
    - **Findings**: the evidence gathered and your conclusions.
    - **Actions**: all steps you took during troubleshooting.
    - **Outcomes**: the results of the troubleshooting process.

CompTIA Troubleshooting Motherboard, RAM, CPUs - Section 5.2

Troubleshooting Steps – Motherboard, RAM, CPUs

Power-on Self-Test (POST) Beeps

- Beep codes vary according to BIOS manufacturer.
- Modern motherboards use LED displays instead of beeping.
- Common causes include:
    - Damaged or improperly seated RAM or GPU
    - CPU issues
    - Failing motherboard components

Blue Screen of Death (BSOD)

- Indicates a critical, non-recoverable error occurred in the system.
    - Common causes include:
        - Failing computer hardware
        - Corrupt or glitchy hardware driver
        - Overheating internal components
        - Faulty PSUs (dirty power)

Black Screen

- The screen may fail to present an image even after attempting to boot.
    - Common causes include:
        - Poorly seated GPU and GPU power connectors
        - Wrong video output used
        - Unplugged power or display cables
        - Wrong display input selected

No Power

- The lack of LED status lights or fan noise indicates a power issue.
    - Common causes include:
        - Power strip not plugged in or switched off
        - Power supply not plugged in or switched off
        - Missing or poorly seated internal power connectors
        - Incorrectly positioned front panel connectors

Sluggish Performance

- The system becomes noticeably slower than usual.
    - Common causes include:
        - Inadequate or failing CPU cooling (thermal throttling)
        - Inadequate airflow through the case
        - Excessive hard drive fragmentation
        - Background tasks (e.g., transient updates)

Overheating

- Overheating PCs often:
    - Slow down (thermal throttling)
    - Randomly shut down (thermal shutdown)
- Common causes include:
    - Poor CPU cooling or case airflow
    - Degraded CPU thermal paste
    - PC location (e.g., enclosed space)
    - High-wattage components in small spaces

Component Failures

- Occasionally, internal components simply fail.
- Indicators of component failure include:
    - Distended or swollen capacitors (they should be cylindrical and not oozing)
    - Burning smells (possible indication of electrical shorts)
    - Grinding noises (failing fans or hard drives)

Inaccurate Date and Time

- The system time becomes inconsistent across reboots.
    - The CMOS battery has died or become unseated, and the internal clock isn’t receiving power.

CompTIA Troubleshooting Drivers and RAID - Section 5.3

Performance Issues

- LED status indicators perpetually lit up:
  - The HDD LED indicators light up when a drive is being accessed.
  - A drive being constantly accessed may indicate read/write issues, or simply being too saturated for its supported speed.
- Extended read/write times:
  - HDD performance is inversely related to disk fragmentation (high fragmentation = slower drive).
  - Excessive read/write latency may also indicate malfunctioning hardware.
- Input/Output Operations per Second (IOPS):
  - Number of discrete read or write operations a storage system can handle per second.
  - Highly fragmented or malfunctioning drives may waste some of the finite IOPS available.

Drive Failures

- A physically failing drive may begin making unusual noises:
  - Grinding and clicking
- Drives may also proactively warn users with SMART errors:
  - Presented during boot or may be identified with certain applications.
- For both physical failures and SMART (Self-Monitoring, Analysis, and Reporting Technology) errors, it is critical to back up as soon as possible (if possible) and replace the drive.

Missing Drives

- "Bootable device not found" errors occur when the BIOS/UEFI can't find a suitable OS to boot.
  - Boot mode (Legacy vs. UEFI)
  - Incorrect boot order
  - Drive not enabled as a boot option
  - Drive issues (e.g., corrupt MBR)
- Secondary drives missing within an OS often indicate:
  - Missing drivers (the OS can't communicate with the drive)
  - The drive needs to be initialized (e.g., via Disk Management)

RAID Troubleshooting

- Drive or data loss on **RAID 0** is not recoverable. No redundancy.
- Drive or data loss on **RAID 1, 5, or 1+0** will slow performance, but replacing the drive allows data recovery.
  - Sometimes the RAID controller fails and must be replaced.