Introduction to CompTIA

Introduction To The CompTIA A+ Certification

- **CompTIA** stands for the **Computing Technology Industry Association**. They are a vendor-neutral non-profit organization that provides **IT certifications**.
- The **CompTIA A+ certificate** is an **entry-level qualification** in the **IT industry**.
- The **A+ certification** consists of **two examinations**:
  1. **The core 1 examination (220-1001)**.
     (a) Mobile Devices.
     (b) Networking.
     (c) Hardware.
     (d) Virtualization and Cloud Computing.
     (e) Network Troubleshooting.
  2. **The core 2 examination (220-1002)**.
     (a) Operating Systems.
     (b) Security.
     (c) Software Troubleshooting.
     (d) Operation Procedures.

Safety and Professionalism

Professional Communication

- **Be on time for meetings**. If you are going to be late, contact the person / people you are meeting and let them know.
- **Actively listen**, make sure that **people understand** that you are **listening** and **avoid interrupting**.
- **Clarify customer statements**, ask **specific questions** to **fully understand problems** people are having.
- Maintain a **positive attitude**, especially if correcting peoples statements.
- Use **proper language**; avoid **jargon, acronyms, and slang**.
- **Set and meet expectations**.
- Be **culturally sensitive**.
- **Don't be judgemental**.
- **Don't argue with customers** and **don't be defensive**.
- **Avoid distractions** when **meeting with people**.

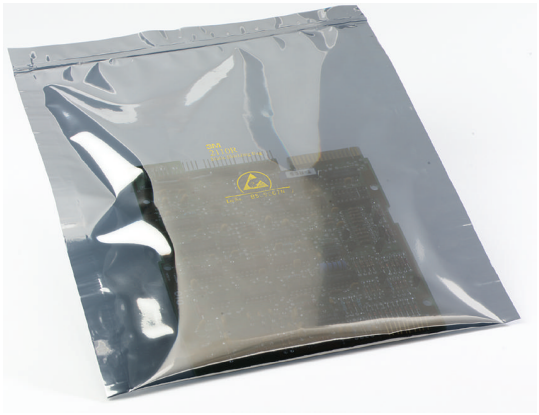
Electromagnetism and Technology

- An **electromagnetic pulse (EMP)** or an **electrostatic discharge (ESD)** can **temporarily or permanently damage electronic equipment** by generating high voltage and high current surges.
  - **Semiconductors** are **at an elivated risk for EMP and ESD damage**.
  - The effects of **EMP and ESD damage** can be range from **being imperceptible to the eye** to **literally blowing devices apart**.

- **Electromagnetic interference (EMI)** is an **unwanted noise** or **interference** in an **electrical path or circuit** that is caused by an **outside source**. EMI can cause electronics to operate poorly, malfunction, or stop working completely.
  - If **EMI** is strong enough, it can **completely wipe hard drives**.
- **Radio frequency interference (RFI)** is **EMI within the radio frequency spectrum**.

Physical Safety

- When **working on hardware** you should always use the **appropriate safety equipment**. This includes masks and safety goggles.
- Always **disconnect electronics from their power source** before performing **repairs**.
- **Electrically sensitive devices** should be **stored in an antistatic bag**.
- When **performing repairs**, devices should be placed on an **antistatic (ESD) mat**.
- The device should be **grounded to the mat**, and you should be wearing an **antistatic (ESD) wrist strap** (must touch skin) that is **also grounded to the mat**.



CompTIA Troubleshooting Theory

- **CompTIA troubleshooting theory** is a **set of steps** that **technicians** can go through to **troubleshoot problems**.
  - There are different approaches to troubleshooting, this is the way that CompTIA prefers.
  - Specific organizations may also have extra steps they want you to perform (eg paperwork).
- **Always consider policies, procedures, and impacts before implementing changes**.
- Troubleshooting steps:
  1. **Identify the problem** — Talk to the user, and discover what issues they are having.
  2. **Establish a theory of probable cause** — Take a look at the device and identify what may be causing the issue.
  3. **Test the theory to determine the cause** — Test the theory to see if it is actually the cause, if it is not, go back to step 2. If you are not able to determine the issue, you can always escalate the problem (ask for help).
  4. **Establish a plan of action to resolve the problem and implement the solution** — Try to resolve the problem.

5. **Verify full system functionality and implement preventative measures if applicable** — Ensure the user is satisfied with the solution and implement preventative measures (this could be telling the user how to prevent the issue, or documenting the issue, or escalating the issues, etc).
6. **Document findings, actions, and outcomes** — This can be organization specific, but document everything that is required.