**CompTIA A+ Core 1**

For a novice low voltage cabling technician preparing for the CompTIA A+ Core 1 exam, there are several key areas to focus on:

1. **Network Hardware and Protocols:** Network components (ie different cable types, connectors), cabling standards, and common protocols (ie network topologies).

2. **Mobile Devices:** Familiarize yourself with laptop components &mobile device connectivity.

3. **Network Troubleshooting:** Study quick-reference tables to diagnose and resolve issues.

4. **Hardware :** Know how to install, configure and maintain hard-drives. Understand personal computer components like CPUs, RAM, motherboards, and power supplies.

5. **Security**: Pay attention to the sections on computer and network security, as maintaining secure connections is a critical aspect of low voltage cabling work[1][2].

<https://hub.totalsem.com> Activity Guide

1. **Self-Protection**

-Disconnect power supply device when necessary

-Attach Electrostatic Discharge Antistatic (ESD) strap to powered device

-Purchase a C-Rated Fire Extinguisher for Electrical Fires

-Lift with Legs, Not with Back -Lift 25lbs+ Devices with Assistance (Use Hand

1. **Tech Tools**

-Voltage Tester -Hemostat -Tweezers -IC Inserter

-Thumb Drives (USB) -Volt/Ohm Meter (Multimeter)

1. **Troubleshooting Methodology**

\*CompTIA A+ defines a specific workflow process to troubleshoot any system problem.

1. Consider Policies, Procedures & Impacts before Implementing Changes
2. Identify the Problem: Inquire with User about Troubles
3. Review System & Application Logs == Escalate Issue
4. Establish a Plan of Action to Resolve Issue & Implement a Solution
5. Verify Full-Functionality (Demonstrate) & Implement Preventative Measures
6. Document Findings, Actions and Outcomes (Share Lessons Learned for Next-Tech)

*Troubleshooting Tools:*

Security-centric Linux Distro VMs <https://www.kali.org/get-kali/#kali-virtual-machines>

Penetration Testing Framework <https://www.metasploit.com/>

Network Security Scanner <https://nmap.org/>

Disk Encryption <https://veracrypt.fr/en/Home.html>

Create Bootable USB Drive <https://rufus.ie/en/>

Network Protocal Analyzer <https://www.wireshark.org/>

Partition Editior <https://gparted.org/>

Memory Testing Tool <https://www.memtest.org/>

Hardware Monitoring <https://www.cpuid.com/softwares/hwmonitor.html>

**Networking Essentials** (Tools, MAC Frame, 568B Wiring, Topologies)

**LAN - Local Area Networking**

-Find IP Address & IP Host -Test Network Connections

-Configure IPv6 and IP in Windows -DNS Names, Records & Hop Count

-Workgroup Settings & Logon -Top Level Domains

-Find Default Gateway, Default DNS Server & Subnet Mask

**The Internet**

-Internet Connections -Protocols & Port Numbers -Clear Browser Data

-Verify a Secure Connection -Connect to a VPN -DNS Cache

**Utility Launch Points:** Control Panel, System/Device Manager and Admin Tools

Install a CPU + Measure RAM Size, DDR Rating and Speed + UEFI BIOS // Motherboard

**Install & Upgrade an Operating System**

-Registry File Location -Performance Monitor -System Root

-Management Console -Task Manager Troubleshooting (tasklist)

**Maintain & Optimize Operating Systems** (Configure Windows Update, Task Scheduler, Disk Cleanup, Managing Applications, Backup Types, Time Machine)

**Working with the Command Line Interface** (dir, cd, md, wildcards, advanced)

**Troubleshooting Operating Systems**

-Create a Restore Point -BCDEdit Utility -Event Viewer / File Checker

-Troubleshooting Drivers -Windows Recovery Environment (WinRE)

**Display Technologies** (Connectors, Settings, DxDiag Utility, Managing Video Drivers)

**Wireless Networking** (Wireless Standards & Technologies, Configuring a WAP)

**Mobile Devices** (Setup Mobile Phone HotSpot, WiFi, Email, and Maintain & Secure)

**Printers & Multifunctional Devices** (Printer Parts, Laser Printer Components, Sharing)

**Securing Computers**

-Scanning Computers to Identify Malware & Phishing Threats

-Securing Wireless Networks

-Remove Viruses (Recognize, Quarintine, Search & Destroy)