THE TROUBLESHOOTING PROCESS: LAYING THE GROUNDWORK

This assignment will begin the process of examining the troubleshooting process as a whole, relating the steps discussed here to the practice of technician work in the field. Although this section of the study unit is primarily focused on the process, there are too many steps to squeeze into one assignment. Instead, this assignment and the ones that immediately follow will break the process into broader categories based on their overall process, and examine them on that basis.

Step 1: Prepare

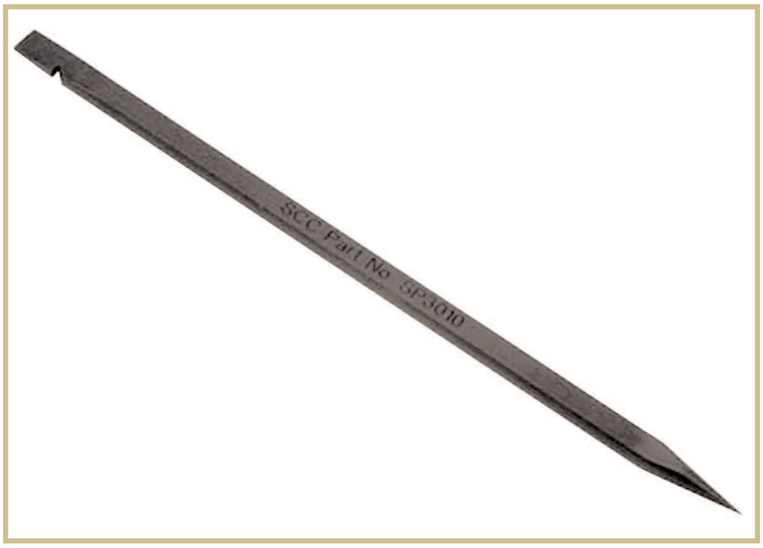
Depending on the organization a technician works for and how technical issues are generally handled, you as a technician may find out about technical issues in a number of ways. In a traditionally structured help desk, you may get a phone call, e-mail, or help desk ticket stating the nature of the issue and, frequently, a sense of its urgency. If you work in a smaller organization, you may get a face-to-face visit, or might be told when making the rounds of the office. For those technicians managed directly, your boss may assign you a set series of issues to look into and fix.

Regardless of how the matter is communicated, though, the process remains the same. Whenever a technician is informed of an issue, the first step of the troubleshooting process is to prepare for the task ahead, which means assembling and/or obtaining the tools the technician will need to address the issue. This tool kit will be defined in part by the nature of the technician's job; if the technician is a help desk employee who doesn't leave the call center, for example, having a multimeter on hand won't be of much use. Similarly, repair technicians who replace and upgrade hardware all day may not have much need for a Windows repair disk. However, most technicians will probably be called upon to regularly perform hardware and software troubleshooting as a matter of course, so in most cases, a tool kit that covers both hardware and software will be necessary.

Although a specific tool kit is best developed over time—and will change, depending on the technician's needs and experience—there are certain parts that go into making an effective all-purpose tool kit. If you as a technician are starting your tool kit for the first time, here are a few tools you'll want to include:

- *Multitool or basic PC set:* Most computer and electronics store sell these, ranging from a small set of screwdrivers, Torx drivers, and tweezers in a leather pouch to deluxe cases that include multiple sets of ratchets, soldering guns, and electronic probes. For the vast majority of hardware work, a *multitool*—commonly called a *Leatherman,* after one of the most popular brands—will suffice. Most PCs are designed to be taken apart with only a Phillips screwdriver, although technicians who do hardware work on Macs often require various Torx drivers and an all-purpose plastic stick for specialized procedures (Figure 4).

FIGURE 4—Apple Nylon Probe Tool



- *Anti-malware software:* With the rise of the Internet and the trend toward Web-based applications, or cloud computing, the dangers of *malware*—software designed specifically to infiltrate, modify, steal, or destroy data and equipment—present an ever-increasing challenge for organizations and technical support staff. In many cases, the issues end users report can be traced back to a malware infection, so having the tools on hand to address malware is vital. A *boot disk* that has antivirus and antispyware scanners is invaluable for this purpose. Some antivirus software can make a boot disk with a scanner installed on it; other options include obtaining a boot disk with a suite of tools on it, such as Microsoft's DaRT or the Knoppix LiveCD, which allows the machine to boot into a shell without engaging the operating system and giving the infection a chance to spread.

- *Operating system installation media:* For some problems, the most effective solution to an issue will be a reinstallation of the operating system. While many organizations maintain image files on servers to streamline this process, plenty of organizations don't, so technicians will often have to do an installation from scratch. In such cases, it will be necessary to have a legal copy of the installation media handy, along with the serial number or registration code. This media can be a CD or DVD, an OEM partition or a network share.

- *Administrative or account passwords:* These are generally necessary in organizations with a private network. Good security practice calls for providing users only the level of rights and privileges needed to do their jobs and no more, which means certain maintenance and configuration tasks on PCs can't be done by end users. To perform such tasks, such as adding a user to a specified group or modifying access permissions, administrative passwords will be needed. Also, access to certain accounts and applications may be needed for testing purposes, particularly when trying to duplicate reported symptoms.

- *Contact information for technical resources/additional assistance:* Issues with applications or hardware may be troubleshot to specific problems that may be outside of a technician's purview or may require specialized knowledge. In such cases, it may be necessary for a technician to contact the support department for a specific vendor to further troubleshoot a problem. Additionally, in some cases, an issue may be a known problem or defect in a product, or there may be an update or hotfix available for it through the vendor.

Step 2: Make a Damage Control Plan

Once the tool kit is assembled, the first step of the troubleshooting process is complete. That doesn't mean, however, it's time to rush off and start poking and prodding at a computer. Part of laying the groundwork for a successful resolution is preparing for worst-case scenarios; due to the complexity and interrelated nature of computer hardware and software, issues that start small can grow with astonishing speed, and while nobody likes to think about the worst that can happen, it's part of the technician's job to know what that can be, and take steps to avoid it.

As a result, the second step in the troubleshooting process is to make a *damage control plan* for the issue at hand. This can be a logical process as detailed as the troubleshooting steps, or it can be a general set of loose guidelines, but the purpose is the same either way: minimize inconvenience and downtime for the end user and the organization. A good damage control plan isn't just for the technician; it involves the end user as well, which both helps the user remain in the loop and helps educate the user on ways to potentially avoid such issues in the future.

The first concern of a damage control plan is to protect the data affected by the issue. This refers not only to the data specifically accessed by an application or function, but all the data stored on the computer itself. Before beginning work on a computer, a technician should always make sure that the machine is backed up—preferably by a tape backup system or a *storage area network (SAN) system* in enterprise networks, an online service or external storage device for individual machines or small organizations—and that the data is safely stored elsewhere. If a backup solution isn't already in place, the technician should consult with the user and make sure all important data—documents, data files, archives, and e-mail—is backed up to an external device or network. A technician should *never* simply assume a user's data is backed up; the damage potential due to data loss is too great, even if the procedure is minor.

Another concern of a damage control plan is user inconvenience. Unless the computer or OS has completely failed, the end user may still be able to work, and may not be able to simply stop work for an undetermined length of time while the technician troubleshoots the machine. Whenever possible, the technician should try to schedule a visit or, in many cases, remote access to the machine at a time when the end user doesn't need to be using the machine: after hours, for example, or during lunch or a meeting. Since troubleshooting OS and/or software issues often requires rebooting or administrative-level access to the machine, working without the user's presence may make the job easier and faster to accomplish.

Having addressed data protection and user inconvenience, there's a third aspect of damage control planning to be considered: protecting the technician from harm. In many production environments, such as industrial workspaces or "clean room" manufacturing areas, it may not be feasible to remove a computer to a repair depot or technician area, meaning the technician may have to work in the presence of large machinery, chemicals, or electrical hazards. On top of these factors, technicians must be careful whenever working inside a computer case to protect the components from *electrostatic discharge (ESD),* or the transfer of electrical charge between differing potentials; in this case, from the technician to the computer. Amounts too small for humans to perceive can damage or destroy electrical components. Simply walking across a carpet can generate up to 10,000 volts of static electricity, but certain electrical components can be damaged with as little as 100 volts.

Thus, technicians must make sure to take the environments where the work will be done into account, particularly in cases where the case must be opened and internal components replaced or accessed. Regardless of environment, any technician working inside the case or with components must wear ESD-safe wrist bands and/or shoe straps, and either attach a ground wire or take care to frequently ground against the table or metal case to discharge static harmlessly. Certain production environments may require the use of goggles, hard hats, gloves, masks, respirators, and full-body suits; before entering the environment, the technician must make sure all the necessary safety equipment is available and in good working order.

Step 3: Get Symptom Description

The steps that have been laid out so far concentrate on preparation, getting what's needed together before digging in. Once the tools are assembled and a damage control plan is in place to protect the user and the technician from worst-case scenarios, it's time to start the part of the process many people think of when troubleshooting is mentioned: finding out what the symptoms are. Part of this step may be handled when the technician is first informed of the issue, but it's important to understand that this aspect is very vital, and deserves its own focus. Over time, as a technician gains in experience, this step may become the first step in the technician's own process—as the first two steps may become automatic—so setting the tone correctly for the user and the organization from the very beginning becomes even more important.

For many troubleshooting incidents, this may be the first point where the technician interacts with the user, so it's important to note both technical and customer service skills will come into play here. Not only is the technician searching for specific symptom-related information and background on specific computer settings, but he or she is also getting a sense of the user's priorities and background information regarding the issue. Sometimes users are reluctant to bring up certain pieces of information for fear of looking unknowledgeable or out of fear of being blamed for the problem; very often, users may have noticed something they don't think is important, but may shed light on the issue. As a result, technicians must do more than obtain technical information; they must actively listen, and understand how to use open-ended questions to get the user to feel comfortable and talk freely about the symptoms.

Before discussing the specific information technicians need to obtain in this step, it should be noted that at this point, any attempt at diagnosis or repair should be put on hold. Trying to act without as complete information as possible can lead a technician down an incorrect resolution path, which can waste time and effort—as well as financial resources—in an attempt to apply a solution to incomplete data. This stage should focus only on symptom and system data. Diagnosing issues will come at a later step.

When discussing the symptoms with the user, or when examining the machine in person or remotely, the technician's focus should be on obtaining as much information as feasible, particularly regarding the system's behavior, to generate a complete and accurate symptom description. To that end, the information needed will include, but isn't limited to, the following:

- *System configuration details,* including the hardware components, the installed applications and the operating, system version. In the case of Windows, this information should include the installed service pack.

- *Specific error message,* if one is being displayed. In some cases, multiple error messages may appear in order; each error message text should be recorded, and the order in which they appear.

- *The actions the user was performing* when the symptoms and/or error messages first appeared, including the active application and what other applications were open but minimized or simply in the background. This should also include any applications that had been triggered but not fully opened, as well as any that were just closed prior to the reported issues.

- *Time frame and frequency of the symptoms.* If the error has just started, that can help narrow down possible causes later. Also, knowing a set period of time in which the error has happened, or the cycle on which errors appear, also helps narrow down potential causes.

- *Reproducibility of the symptoms,* as being able to reproduce the symptoms at will is a useful tool for troubleshooting. It helps point to potential causes or mitigating factors, and offers a way to test the symptom occurrence in a more controlled environment.

Once this information is gathered, a technician may be tempted to charge into troubleshooting, especially if the technician is experienced and suspects he or she knows what the problem is based on past experience. This is an understandable reaction; it's also a bad one to act on, as it can potentially lead to drastic errors and wasted time. Your hunch about a technical problem or symptom may be spot on, but it may not be. Investing a little extra time in the beginning steps of the process will save a great deal of time on the other end, and be of more worth to your users in the long run.

Take time now to complete *Self-Check 3* before covering the next steps in the troubleshooting process.

Self-Check 3

1. What is the first concern of a damage control plan?

2. How much voltage is required to destroy some electrical components?

3. When discussing symptoms with an end user, a technician must employ ________ and ________ skills.

4. *True or False?* Every technician's tool kit should contain a soldering iron.

5. *True or False?* Technicians should always note which service pack is installed on a Windows machine.

Check your answers with those on page 65.