

ITFreeTraining



CompTIA Troubleshooting Model

For the free video please see
<http://itfreetraining.com/ap/1e20>

In this video from ITFreeTraining, I will look at the CompTIA Troubleshooting model. Once you get some experience troubleshooting, you will develop your own methods, but the CompTIA Troubleshooting model gives you a good framework to work with, particularly when you are new to troubleshooting.

The image is a screenshot of the CompTIA website. At the top left is the CompTIA logo. To its right is the title "Troubleshooting Model" in a large white font. Below the title is a navigation menu with links for "Certifications", "Training", "Testing", "Continuing Education", "Events", "Resources", and "Members". In the top right corner, there are "Login" and "Store" buttons. The main content area features a list of six steps for the troubleshooting model, numbered 1 through 6, in white text on a blue background. The steps are: 1. Identify the problem, 2. Establish a theory of probable cause, 3. Test the theory to determine cause, 4. Establish a plan of action and implement, 5. Verify full system functionality, and 6. Document findings, actions and outcomes. Below the list, there are three columns for different certifications: "CompTIA A+", "CompTIA Network+", and "CompTIA Security+". Each column has a brief description of the certification's value.

CompTIA Troubleshooting Model

1. Identify the problem
2. Establish a theory of probable cause
3. Test the theory to determine cause
4. Establish a plan of action and implement
5. Verify full system functionality
6. Document findings, actions and outcomes

CompTIA A+ CompTIA Network+ CompTIA Security+

A+ is the starting point for a career in IT. The performance-based exams certify...
Network+ certifies the essential skills needed to confidently design, configure, and troubleshoot...
Security+ provides a global benchmark for best practices in IT network and...
Get the skills you want and employers need.

0:16 The CompTIA Troubleshooting model has six different steps. These are: identify the problem; establish a theory or probable cause; test the theory; establish a plan of action and implement; verify full system functionality; document findings, actions and outcomes.

Although you will most likely develop your own style about how to fix problems, this gives a basic framework on how to look at problems. I will now have a look at each of these steps individually.

Identify the Problem

- Question user and identify user changes to computer
- Perform backups before making changes
- Inquire regarding environmental/infrastructure changes
- Review system and application logs



Level	Source	Event ID	Task Category
Warning	DistributedCOM	10016	None
Warning	DistributedCOM	10016	None
Warning	DistributedCOM	10016	None
Warning	DistributedCOM	10016	None
Warning	DistributedCOM	10016	None
Warning	DistributedCOM	10016	None
Information	Kernel-General	16	None
Information	Kernel-General	16	None
Information	Kernel-General	16	None
Information	Eventlog	6013	None
Information	Service Control Manager	7040	None
Information	Service Control Manager	7040	None
Warning	DistributedCOM	10016	None
Warning	DistributedCOM	10016	None
Information	Service Control Manager	7040	None
Information	Service Control Manager	7040	None
Warning	DistributedCOM	10016	None

0:48 The first step is to identify the problem. Generally, you are attending a user's computer because they have reported something is wrong. This will normally be because they are not able to do something and it has stopped them from working effectively; however, it may not be the source of the problem. The problem could be anywhere, such as software on the computer, software on the network or internet, or perhaps the user is just not doing something the right way.

The first step is to question the user. You first want to establish what they are doing and what is happening. Start asking questions such as the following, "Have you attempted to do this before?" If they say they do the same thing every day, you know that potentially something has changed. Next, we need to find out what that change is.

In computing, you may find that something has broken because the user did something to the computer. This does not happen as often nowadays as businesses generally reduce the amount of access a user has to the computer, so essentially, they cannot break as many things as they used to be able to. You do need to be careful how you word the questions. You don't want to assume that they have changed something; however, you don't want to not ask that question either. So, when dealing with customers, remember it is not what you say, but it is how you say it. Asking the question "Have there been any recent changes made to the computer?" is a better question to ask than "What have you done to the computer to break it?" Remember you don't want to come across as rude or accusative when you talk to them; all you want is the information to help you solve the problem, and you get that information by using some good communication skills. Remember: The customer is the reason that you have a job.

In some cases, you will find that the user will not give you the information straight away. So, you may have to be careful and ask the question a few different ways. For example, if they are not giving you anything straight away, maybe ask a different question such as “Has additional software been installed or have there been any updates recently?” This is where you may get an answer along the lines of, “I got some message this morning and I just pressed O.K., does that have anything to do with it?” They may not know what this message was but may be able to describe when they got it and/or what it looked like. This will give you an idea of where to look.

Let’s consider an example. An update has been pushed out by the manufacturer of the software which has broken the software. Remember, the users are not always the most technical people. They may also not have a good understanding of what is happening, so it may take a little time to get the information out of them. They are not doing this on purpose, and we should have a little patience with them and not be accusative or angry if it takes a little bit of time.

Before we start making any changes, we want to perform a backup to make sure that we don’t lose anything. For the CompTIA exam, we always backup everything before we make changes. In the real world, we don’t do this for every job. We only make backups when we need to. Many businesses have their workstations set up so all the users’ data is stored on the network rather than the local computer. Thus, no need for backups for most activities.

Sometimes you will find that some settings or files will be stored on the local computer or in other strange places. I once had a user store all their files in the Windows temp folder. When I asked them why they stored them there, they told me this was the folder that appeared when they started using the computer so they kept using it. I can only assume the person setting up the computer stored something in the temp folder before giving it to the user and the computer remembered this location. The user then simply kept using this folder as it was the folder that first appeared. If you choose not to make a backup, keep in mind that, if you start deleting things, you won’t necessarily be able to get these things back. You don’t want to delete all the user’s important documents because they saved them in the wrong place. If you are not sure, simply move them to a different folder first and see if this affects anything.

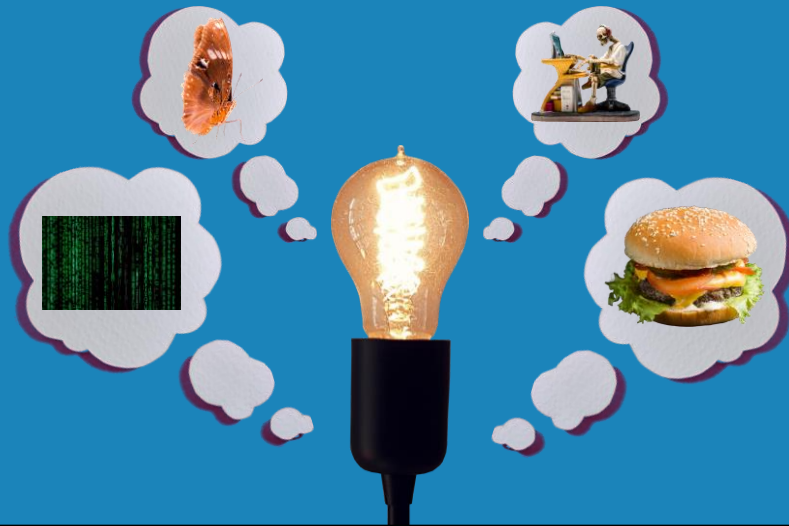
The next question you want to ask is, “Has there been an environmental or infrastructure change recently?” This is where you may find out things like, there were some IT guys working in the network cabinet earlier today. Sometimes we make changes on the network without telling each other. Other times, they may say things

like, "I moved departments the other day." This may be as simple as moving their computer from one side of the room to the other, however on some networks this may cause problems. For this example, let's say the user has changed departments and they let IT know this was occurring. Since they have only just changed departments, they are still doing some work for their old department and thus need to use software from the that department; however, this software is no longer working.

The next step is to review the application and system logs. This will give you an idea of what is happening with the computer. If we know when the problem started occurring, we can see if there are any strange error messages in the log at that time. In this example, a strange error message appeared at the time when the problem started occurring. I wonder if this could be related to the problem that we are having.

Establish a Theory of Probable Cause

- Taking a guess what is wrong



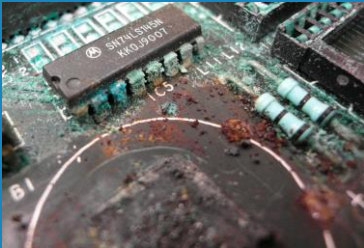
6:07 The next step is to establish a theory for the probable cause of the problem, essentially taking a guess at what is wrong. In order to do this, consider the symptoms of what is occurring. For example, the user is saying the computer has started running slowly and this was probably caused by something having changed. In some cases, this may be a hardware problem. Have a look around the computer for damaged or broken cables. If you open the computer, have a look to see if anything looks damaged. If there is a large amount of heat inside the computer then probably one of the fans has stopped working.

When looking for problems, use all your main senses. Listen to the computer, and if you hear clicking noises or other unusual sounds this may indicate there is a problem with the hardware in the computer. Electronics give off an electrical smell when they are damaged and are shorting out. If you notice that smell, you know that something is damaged inside the computer or soon will be.

Your research into the problem may also include doing some internet searches or searching through your on-site documentation. If you have an error code, these are always good items to search for. This could be either an error the application has given you or one you have found in the system logs. Once you have your information together, you have a theory of probable cause or at least a good guess at what the problem is.

Test the Theory to Determine Cause

- Verify the cause
 - Otherwise, come up with a new theory
- Get permission if required to fix
- Escalate the problem otherwise



7:32 The next step is to test your theory to determine if it is the cause. In some cases, it may be verifying that a part is broken. In our example, the problem is that a Windows update is causing a conflict with the software. This was not a problem until the software was updated. We have verified the software version and the particular Windows update on the computer that is causing the problem.

If you find that your theory is not what was causing the problem, come up with a new theory to what the problem may be.

Once you establish what is wrong, you may need to get permission to fix it. This may mean speaking to your manager or putting in a request to get something changed. In our example, the simple solution is to remove one of the updates, either the software or the Windows update. However, which do we remove? In this case, we need to remove the Windows update as the software will no longer work if the update is installed. Windows updates in this case are managed. If we did remove it, the network management software would detect it has been removed and would re-install it, putting us back in the same position.

In some cases, you may need to escalate the problem. In other cases, you may know what the problem is, but don't have the access or skills to fix the problem. This is common practice in companies, so nothing to worry about. There will be a procedure that you will need to follow in order to escalate the problem. Escalating the problem can also include contacting suppliers, manufacturers or using websites. Sometimes posting the problem you are having on-line will get a response back quite quickly, but not always.

Establish a Plan of Action and Implement

- What permission/resources are required?
- Remember to backup data



9:10 The next step is to work out a plan. In your plan you should consider what permissions you require and what resources you need. Many companies will have procedures and processes in place that determine how you can make changes to the network. If you require any parts, are they available or do you need to order them first? There is not much point taking a user's semi-working computer apart, effectively making it no longer usable, then telling them it will be a week before you get the part; you may as well leave it in one piece until the part arrives.

Often your plan will fall into one of three different categories. These are: repair, replace or workaround. A lot of the time this will be a balance between cost and repair times. Often it is better for a company to replace a malfunctioning computer rather than spending the time trying to work out what the problem is. However, if the computer is a specialized workstation that costs a lot of money then this will not be an option and you will need to fix it.

Remember as well, before you implement your plan, backup any data that you need. In the real world, depending on what you are doing, there may be no need to back anything up, but in the case of the exam, we always backup our data.

Verify Full System Functionality

- Generally get the user to confirm



10:28 The next step is to verify that everything is working. It is a bit embarrassing if you say everything is fixed and a few minutes later you get a phone call saying it is still not working. After you have tested it yourself, generally it is a good idea to get the user to confirm the problem is fixed when appropriate. This is particularly the case when they are using a specialized software application. The user will know how to use the application and can quickly tell you if it is working o.k. or not.

Document Findings, Actions and Outcomes

- Document in company knowledge base
- At least document for yourself



10:58 The last step is to document your findings, actions and outcomes. If possible, do this in your company's knowledge base. This will allow other technicians to find the documentation if they have the same problem. There is nothing worse than spending a lot of time trying to find a solution to a problem and then have someone say, oh I had the same problem last week. That would have been useful knowledge to have had earlier.

The information is also useful if the same problem seems to be occurring over and over again. If you observe that a particular computer keeps having strange problems repeatedly, maybe it is time to replace that computer rather than spending the time trying to troubleshoot. It may be cheaper for the company to retire a computer earlier, rather than repeatedly trying to fix it.

If you are not able to document the problem in the company's knowledge base, you should at least document it for yourself. In a year's time, if you come across the same problem again, hopefully you will remember how to fix it. If the answer is you can't remember, spending a minute making some notes now will be a big-time saver in a year's time. You don't want to waste time troubleshooting the same problem twice.

That covers it for the CompTIA Troubleshooting model. In the real world, having a methodical process like this is ideal; however, you will find that often problems are time-critical. This means the technician needs to often strike a balance between being methodical and being efficient. Once you start getting some experience, you will work out your own way of doing things, but at least when you are starting out, the troubleshooting model gives you a step-by-step process of how to go about fixing problems.

I hope you have enjoyed this video from ITFreeTraining and have found it informative. For more free videos from us, please see our YouTube channel or website. Until the next video, I would like to thank you for watching.

References

“The Official CompTIA A+ Core Study Guide (Exam 220-1001)” Chapter 3 Position 15550-18739

“CompTIA A+ Certification exam guide. Tenth edition” Pages 18-24

“Picture: Question mark” <https://www.pexels.com/photo/ask-blackboard-chalkboard-chalkboard-356079/>

“Picture: Questions Answers” <https://www.pexels.com/photo/questions-answers-signage-208494/>

“Picture: Tape” <https://www.pexels.com/photo/black-cassette-tape-on-white-wooden-table-1393318/>

“Picture: Different shoes” <https://www.pexels.com/photo/man-person-legs-grass-539/>

“Picture: Light blub” <https://www.pexels.com/photo/turned-on-pendant-lamp-132340/>

“Picture: Balloon” <https://www.pexels.com/photo/white-bubble-illustration-1111372/>

“Picture: Internet abstract” <https://www.pexels.com/photo/working-pattern-internet-abstract-1089438/>

“Picture: Butterfly” <https://www.pexels.com/photo/brown-butterfly-2232497/>

“Picture: Computer figure” <https://www.pexels.com/photo/computer-earphone-figurine-furniture-463684/>

“Picture: PCB corrosion” https://commons.wikimedia.org/wiki/File:PCB_corrosion.jpg

“Picture: Yes” https://unsplash.com/photos/__Hw50q04FI

“Picture: Escalator” <https://www.pexels.com/photo/photo-of-escalator-and-staircase-1756251/>

“Picture: Paper note” <https://www.pexels.com/photo/white-paper-with-note-669986/>

“Picture: Checklist” <https://www.pexels.com/photo/banking-business-checklist-commerce-416322/>

Credits

Trainer: Austin Mason <http://ITFreeTraining.com>

Voice Talent: HP Lewis <http://hplewis.com>

Quality Assurance: Brett Batson <http://www.pbb-proofreading.uk>