Network Troubleshooting Methodology

by Sophia

WHAT'S COVERED

In this lesson, you will learn a seven-step network troubleshooting methodology. We will also introduce a number of network troubleshooting tips that may help you to quickly resolve technical issues.

Specifically, this lesson will cover the following:

1. Seven-Step Troubleshooting Methodology

Network troubleshooting is best done by adhering closely to a formal methodology. A **methodology** can be defined as a collection of methods, practices, procedures, and rules used by those who work in some field. Using the seven-step methodology described here may help you to resolve network issues quickly and efficiently.

TERM TO KNOW

Methodology

A collection of methods, practices, procedures, and rules used by those who work in a certain field.

1a. Step 1: Identify the Problem

Before you can solve a problem, you typically will need to **troubleshoot** the problem by figuring out what the problem is. Asking the right questions can get you far along this path and really help clarify the situation. Identifying the problem involves steps that together constitute information gathering.

FORMULA TO KNOW

A good way to start is by asking the user experiencing the problem questions like the following:

- Which resource are you not able to access?
  - The internet?
  - A particular website?
  - A certain file?
  - A type of service?
  - None of it at all?
- Are you able to use your web browser?
- Are you able to duplicate the problem?
- If the problem has to do with an internal server, check to see if you able to ping the server. If this works, then teach the user how to do this.
- Finally, check to see if the user has access to a telnet or FTP to an internal server. If they do, help the user verify local network connectivity.

HINT

If there are multiple complaints of problems occurring, look for the big stuff first, then isolate and approach each problem individually.

When a user reports an issue, you should attempt to duplicate the issue. When this is possible, it will help in discovering the problem. When you cannot duplicate the issue, your challenge becomes harder because you are dealing with an intermittent problem. These issues are difficult to solve because they don't happen consistently.

Do your best to determine if anything has changed. If you can reproduce the problem, your next step is to verify what has changed and how.

EXAMPLE Drawing on your knowledge of networking, you ask yourself and your user questions like these:

- Were you ever able to do this?
- If so, when did you become unable to do it?
- Has anything changed since the last time you could do this?
- Were any error messages displayed?

- Are other people experiencing this problem?
- Is the problem always the same?

TERM TO KNOW

Troubleshoot

To analyze or diagnose a problem or something faulty to the point of determining a solution.

1b. Step 2: Establish a Theory of Probable Cause

After you observe the problem and identify the symptoms, the next step is to establish its most probable cause. You need to come up with at least one possible cause, even though it may not be correct. And you don't always have to come up with it yourself. Someone else in the group may have the answer. Also, remember to check online sources and vendor documentation.

Understand that there are lots of problems that can occur on a network, which could include, but not be limited to the following:

- Port speed
- Port duplex mismatch
- Mismatched maximum transmission unit (MTU)
- Incorrect virtual local area network (VLAN)
- Incorrect IP address/duplicate IP address
- Wrong gateway
- Wrong domain name system (DNS)
- Wrong subnet mask
- Incorrect interface/interface misconfiguration
- Duplicate MAC addresses
- Expired IP address
- Rogue domain name system (DHCP) server
- Untrusted Secure Sockets Layer (SSL) certificate
- Incorrect time
- Exhausted DHCP scope
- Blocked TCP/UDP ports
- Incorrect host-based firewall settings
- Incorrect ACL settings
- Unresponsive service

Many of the problems listed above happen because a device has been improperly configured. You may find helpful information in the configuration guide for your hardware.

1c. Step 3: Test the Theory to Determine Cause

Once you've gathered information and established a plausible theory, you need to determine the next steps to resolve your problem. When the testing of the theory is complete, you will have determined if the suggested cause is correct. If you find you are correct, the next step is to establish a plan of action to resolve the problem and identify potential effects.

If you find that the suggested theory is not the cause of the issue, then you should move on to test any other theories you may have developed. When you have exhausted all theories you have developed, escalate the issue to a more senior technician or, when it involves a system with which you are unfamiliar, the system owner or manager.

1d. Step 4: Establish a Plan of Action to Resolve the Problem and Identify Potential Effects

Identify some possible configuration changes to resolve the problem, and then follow through and test your solutions to see if they work. Once your solution seems to work, test the proposed solution on the computer of the user who is waiting for a solution. If the user is satisfied that the problem is resolved, all is well. If not, go back to step 2, select a new possible cause, and redo step 3.

HINT

If this happens, keep track of what worked and what didn't, so you don't make the same mistake twice.

1e. Step 5: Implement the Solution or Escalate as Necessary

Now that you have determined what the problem is, you need to resolve the problem for all affected users. And if you can't fix the problem, you should know how to escalate it and to whom. Resources to help you in this process include your own problem-solving skills, reference-oriented technical books, the internet, or even an expert at the vendor's technical support center.

Below is a list of complex issues that a junior network technician may need to escalate to a senior network engineer who has the additional experience and knowledge required to resolve the problems:

- Switching loops
- Missing routes
- Routing loops
- MTU black hole
- Bad hardware modules
- Proxy Address Resolution Protocol (ARP)
- Broadcast storms
- Network interface card (NIC) teaming misconfiguration
- Power failures/power anomalies

If your solution seems to fix the problem, then proceed to step 6.
If you can't implement a solution and instead have to escalate the problem, there is no need for you to go on with steps 6 and 7 of the seven-step troubleshooting model. Instead, meet with the emergency response team

to determine the next step.

1f. Step 6: Verify Full System Functionality, and if Applicable, Implement Preventative Measures

After you have executed your solution to solve a network problem, be sure to carefully test the network to verify that your solution actually fixed the problem. Once you have verified that the issue has been corrected, then spot check the network to look for any new problems that your solution may have caused. Use your network troubleshooting tools to verify proper network functionality, and then follow up with the individual users who initially reported the problem to have them verify that the network is working correctly for them.

A mistake that a network technician might make is to solve one problem and think it is fixed without stopping to consider the possible consequences of the solution. Occasionally, fixing one problem may cause other functions or features to break. So before you fully implement a solution, make sure you thoroughly understand the ramifications of their actions.

1g. Step 7: Document Findings, Actions, and Outcomes

Accurate network documentation is vital to the success of any information technology operation. Always document problems and solutions so that you have the information at hand when a similar problem arises in the future. With documented solutions to documented problems, you can assemble your own database of information that you can use to troubleshoot other problems.

Be sure to include information like the following:

- A description of the conditions surrounding the problem
- The OS version, the software version, the type of computer, and the type of NIC
- Whether you were able to reproduce the problem
- The various solutions you tried
- The ultimate solution

Documentation can consist of an up-to-date network map, receipts for network equipment, a collection of owner's manuals and configuration guide, a spreadsheet to record services, changes, network-addressing assignments, access lists, and so on. Just a small number of key documents may save lots of time and money and prevent frustration, especially at the critical time when you are working to solve a network outage.

---

2. Troubleshooting Tips

Now that you've learned the basics of network troubleshooting, let's review some troubleshooting tips for you to consider when you need to create a technical solution to a challenging problem.

2a. Start Troubleshooting From Layer 1

Many network issues are caused by a physical problem at Layer 1 of the OSI Reference Model, like power cords not plugged in, broken network cables, and electromagnetic interference generated by various sources in the physical environment. Therefore, you should generally start your troubleshooting process with the physical components that reside in Layer 1, and then work up the layers sequentially from there.

BIG IDEA

Many network problems are caused by physical issues so start your troubleshooting process at Layer 1 (Physical) of the OSI Model and work up the layers sequentially from there.

2b. Don't Overlook the Small Stuff

Remember that problems are often caused by little things like a bad power switch; a power switch in the wrong position; a card or port that's not working, indicated by a link light that's not lit; or simply, operator error. Even the most experienced system administrator has forgotten to turn on the power, left a cable unplugged, or mistyped a username and password. And make sure that users get effective training for the systems they use. Good training should dramatically decrease problems caused by user errors.

2c. Prioritize Your Problems

Being a network administrator or technician can keep you busy, and it's typical to receive multiple calls for help at once. So, you've got to prioritize and handle the most urgent problem first.

You would start this process by asking some basic questions to determine the severity of the problem being reported. Clearly, if the new call is about something little and you already have a huge issue to deal with, you should put the new call on hold or get their info and get back to them later. If you establish a good set of priorities, you'll make much better use of your time.

Here's an example of the rank you probably want to give to networking problems, from highest priority to lowest:

- Total network failure (affects everyone)
- Partial network failure (affects small groups of users)
- Small network failure (affects a small, single group of users)
- Total workstation failure (single user can't work at all)
- Partial workstation failure (single user can't do most tasks)
- Minor issue (single user has problems that crop up now and then)

Because every business context is unique, mitigating circumstances can change the order of this list for any given organization.
Small-scale problems are not always easier to deal with. You may be able to bring up a crashed server in minutes, whereas a user who doesn't know how to make columns line up in Microsoft Word could take a big chunk out of your day. You'd want to put the latter problem toward the bottom of the list because of the time involved. It's generally more efficient to solve problems for a big group of people than to fix one user's problem immediately.

Many network administrators manage all network-service requests by using support-call tracking software, the only function of which is to track and prioritize all network and computer problems.

2d. Check the Software Configuration

Occasionally, network problems can be traced to software configuration, so when you're checking for software problems, don't forget to check types of configurations:

- DNS
- DHCP
- HOSTS file
- Registry
- Application software settings

2e. Don't Overlook Physical Conditions

You want to make sure that from a network-design standpoint, the physical environment for a server is optimized for placement, temperature, and humidity. When troubleshooting an obscure network problem, don't forget to check the physical conditions under which the network device is operating. Check for problems like these:

- Excessive heat
- Excessive humidity (condensation)
- Low humidity (leads to electrostatic discharge [ESD] problems)
- Electromagnetic interference (EMI) and radio frequency interference (RFI) problems
- Power problems
- Unplugged cables
- Cable Problems

SUMMARY

In this lesson, you learned more about troubleshooting, including a systematic approach using a **seven-step troubleshooting methodology** to help find solutions to most of the problems you'll run into in networking. You also learned about some resources you can use during the troubleshooting process. In addition, you learned how important documentation is to the health of your network. Finally, you learned some tips to further prepare you, including **troubleshooting tips** about prioritizing issues, checking for configuration issues, and considering environmental factors. As you venture out into the real world, keep these tips in mind; along with your own personal experience. They'll really help make you an expert troubleshooter.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Methodology

A collection of methods, practices, procedures, and rules used by those who work in a certain field.

Troubleshoot

To analyze or diagnose a problem or something faulty to the point of determining a solution.