Troubleshooting Process

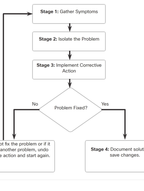
TOPIC

General Troubleshooting Procedures

Troubleshooting can be time consuming because networks differ, problems differ, and troubleshooting experience varies. However, experienced administrators know that using a structured troubleshooting method will shorten overall troubleshooting time.

Therefore, the troubleshooting process should be guided by structured methods. This requires well defined and documented troubleshooting procedures to minimize wasted time associated with erratic hit-and-miss troubleshooting. However, these methods are not static. The troubleshooting steps taken to solve a problem are not always the same or executed in the exact same order.

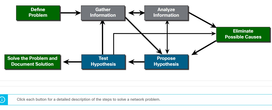
There are several troubleshooting processes that can be used to solve a problem. The figure displays the logic flowchart of a simplified three-stage troubleshooting process. However, a more detailed process may be more helpful to solve a network problem.



TOPIC

Seven-Step Troubleshooting Process

The figure displays a more detailed seven-step troubleshooting process. Notice how some steps interconnect. This is because, some technicians may be able to jump between steps based on their level of experience.



Click each button for a detailed description of the steps to solve a network problem.

Define the Problem	**Define the Problem**
Gather Information	The goal of this stage is to verify that there is a problem and then properly define what the problem is. Problems are usually identified by a symptom (e.g., the network is slow or has stopped working). Network symptoms may appear in many different forms, including alerts from the network management system, console messages, and user complaints.
Analyze Information	While gathering symptoms, it is important to ask questions and investigate the issue in order to localize the problem to a smaller range of possibilities. For example, is the problem restricted to a single device, a group of devices, or an entire subnet or network of devices?
Eliminate Possible Causes	In an organization, problems are typically assigned to network technicians as trouble tickets. These tickets are created using trouble ticketing software that tracks the progress of each ticket. Trouble ticketing software may also include a self-service user portal to submit tickets, access to a searchable trouble tickets knowledge base, remote control capabilities to solve end user issues, and more.
Propose Hypothesis	
Test Hypothesis	
Solve the problem	

TOPIC

Question End Users

Many network problems are initially reported by an end user. However, the information provided is often vague or misleading. For example, users often report problems such as "the network is down", "I cannot access my email", or "my computer is slow".

In most cases, additional information is required to fully understand a problem. This usually involves interacting with the affected user to discover the "who", "what", and "when" of the problem.

The following recommendations should be employed when communicate with user:

- Speak at a technical level they can understand and avoid using complex terminology.
- Always listen or read carefully what the user is saying. Taking notes can be helpful when documenting a complex problem.
- Ask questions to clarify the problem. Avoid telling them how you will help them solve their problem. Users reporting a problem may be under stress and anxious to resolve the problem as quickly as possible.

When interviewing the user, guide the conversation and use effective questioning techniques to quickly ascertain the problem. For instance, use open questions (i.e., requires detailed responses) and closed questions (i.e., yes, no, or single word answers) to discover important facts about the network problem.

The table provides some questioning guidelines and sample open-ended and closed questions.

When done interviewing the user, repeat your understanding of the problem to the user to ensure that you both agree on the problem being reported.

Guidelines	Example Open-Ended End-User Questions
Ask pertinent questions.	• What does not work? • What exactly is the problem? • What are you trying to accomplish?
Determine the scope of the problem.	• Who does this issue affect? Is it just you or others? • What device is this happening on?
Determine when the problem occurred / occurs.	• When exactly does the problem occur? • Does it happen every time? • Were there any error messages displayed?
Determine if the problem is constant or intermittent.	• Can you reproduce the problem? • Can you send me a screenshot or video of the problem?
Determine if anything has changed.	What has changed since the last time it did work?
Use questions to eliminate or discover possible problems.	• What works? • What does not work?

TOPIC

Gather Information

To gather symptoms from suspected networking device, use Cisco IOS commands and other tools such as packet captures and device logs.

The table describes common Cisco IOS commands used to gather the symptoms of a network problem.

Command	Description
`ping` [host] [ip-address]	• Sends an echo request packet to an address, then waits for a reply • The host or ip-address variable is the IP alias or IP address of the target system
`traceroute` destination	• Identifies the path a packet takes through the networks • The destination variable is the hostname or IP address of the target system
`telnet` [host] [ip-address]	• Connects to an IP address using the Telnet application • Use SSH whenever possible instead of Telnet
`ssh -l` user-id ip-address	• Connects to an IP address using SSH • SSH is more secure than Telnet
`show ip interface brief` `show ipv6 interface brief`	• Displays a summary status of all interfaces on a device • Useful for quickly identifying IP addressing on all interfaces.
`show ip route` `show ipv6 route`	Displays the current IPv4 and IPv6 routing tables, which contains the routes to all known network destinations
`show protocols`	Displays the configured protocols and shows the global and interface-specific status of any configured Layer 3 protocol
`debug`	Displays a list of options for enabling or disabling debugging events

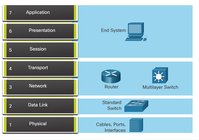
Note: Although the **debug** command is an important tool for gathering symptoms, it generates a large amount of console message traffic and the performance of a network device can be noticeably affected. If the **debug** must be performed during normal working hours, warn network users that a troubleshooting effort is underway, and that network performance may be affected. Remember to disable debugging when you are done.

TOPIC

Troubleshooting with Layered Models

The OSI and TCP/IP models can be applied to isolate network problems when troubleshooting. For example, if the symptoms suggest a physical connection problem, the network technician can focus on troubleshooting the circuit that operates at the physical layer.

The figure shows some common devices and the OSI layers that must be examined during the troubleshooting process for that device.



Notice that routers and multilayer switches are shown at Layer 4, the transport layer. Although routers and multilayer switches usually make forwarding decisions at Layer 3, ACLs on these devices can be used to make filtering decisions using Layer 4 information.

TOPIC

Structured Troubleshooting Methods

There are several structured troubleshooting approaches that can be used. Which one to use will depend on the situation. Each approach has its advantages and disadvantages. This topic describes methods and provides guidelines for choosing the best method for a specific situation.

Click each button for a description of the different troubleshooting approaches that can be used.

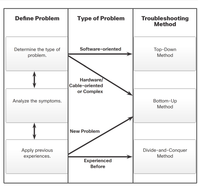
Bottom-Up	**Bottom-Up**
Top-Down	In bottom-up troubleshooting, you start with the physical layer and the physical components of the network as shown in the figure, and move up through the layers of the OSI model until the cause of the problem is identified.
Divide and Conquer	Bottom-up troubleshooting is a good approach to use when the problem is suspected to be a physical one. Most networking problems reside at the lower levels, so implementing the bottom-up approach is often effective.
Follow the Path	The disadvantage with the bottom-up troubleshooting approach is it requires that you check every device and interface on the network until the possible cause of the problem is found. Remember that each conclusion and possibility must be documented so there can be a list of paper work associated with this approach. A further challenge is to determine which devices to start examining first.
Substitution	
Comparison	
Educated Guess	

TOPIC

Guidelines for Selecting a Troubleshooting Method

To quickly resolve network problems, take the time to select the most effective network troubleshooting method.

The figure illustrates which method could be used when a certain type of problem is discovered.



For instance, software problems are often solved using a top-down approach while hardware-based problem are solved using the bottom-up approach. New problems may be solved by an experienced technician using the divide and conquer method. Otherwise, the bottom-up approach may be used.

Troubleshooting is a skill that is developed by doing it. Every network problem you identify and solve gets added to your skill set.

TOPIC

Check Your Understanding - Troubleshooting Process

Check your understanding of troubleshooting processes by choosing the BEST answer to the following questions.

1. Which option lists the three troubleshooting stages in the correct order?

- Gather symptoms, implement corrective action, and isolate the problem.
- (selected) Gather symptoms, isolate the problem, and implement corrective action.
- Implement corrective action, gather symptoms, and isolate the problem.
- Implement corrective action, isolate the problem, and gather symptoms.
- Isolate the problem, gather symptoms, and implement corrective action.
- Isolate the problem, implement corrective action, and gather symptoms.

2. In which step of the seven-step troubleshooting process, would you create a rollback plan identifying how to quickly reverse a solution?

- Analyze information
- Define the problem.
- Eliminate possible causes.
- Gather information
- Propose Hypothesis
- Solve the problem and document solution
- (selected) Test hypothesis

3. Which are recommendations to be used when communicate with a user?

- Always be considerate and empathize with users.
- Always listen or carefully read what the user is saying.
- Speak at a technical level they can understand.
- (selected) All the above

4. During the gathering information step, which command would display the *configured protocols* and the *global and interface-specific status of any configured Layer 3 protocol*?

- show interface
- show ip interface brief
- show ip protocols
- (selected) show protocols
- show section

5. What is the highest OSI layer that should be correlated when troubleshooting routers and Layer 3 switches?

- Layer 1
- Layer 2
- Layer 3
- (selected) Layer 4
- Layer 7

6. Which structured troubleshooting method should be used when a cabling problem is suspected?

- (selected) Bottom-up Troubleshooting Method
- Comparison Troubleshooting Method
- Divide-and-conquer Troubleshooting Method
- Educated Guess Troubleshooting Method
- Follow-the-Path Troubleshooting Method
- Top-down Troubleshooting Method

7. Which structured troubleshooting method should be used when a software orientated problem occurs?

- Bottom-up Troubleshooting Method
- Comparison Troubleshooting Method
- Divide-and-conquer Troubleshooting Method
- Educated Guess Troubleshooting Method
- Follow-the-Path Troubleshooting Method
- (selected) Top-down Troubleshooting Method

Check | Show Me | Reset