Troubleshooting Overview

Internetworks come in a variety of topologies and levels of complexity—from single-protocol, point-to-point links connecting cross-town campuses, to highly meshed, large-scale wide-area networks (WANs) traversing multiple time zones and international boundaries. The industry trend is toward increasingly complex environments, involving multiple media, multiple protocols, and often interconnection to “unknown” networks.

As a result, the potential for connectivity and performance problems in internetworks is high, and the source of such problems is often elusive. The goal of this publication is to help you isolate and resolve the most common connectivity and performance problems for your network environment.

Symptoms, Problems, and Solutions

Failures in internetworks are characterized by certain symptoms. These symptoms might be general (such as clients being unable to access specific servers) or more specific (routes not in routing table). Each symptom can be traced to one or more problems or causes by using specific troubleshooting tools and techniques. Once identified, each problem can be remedied by implementing a solution consisting of a series of actions.

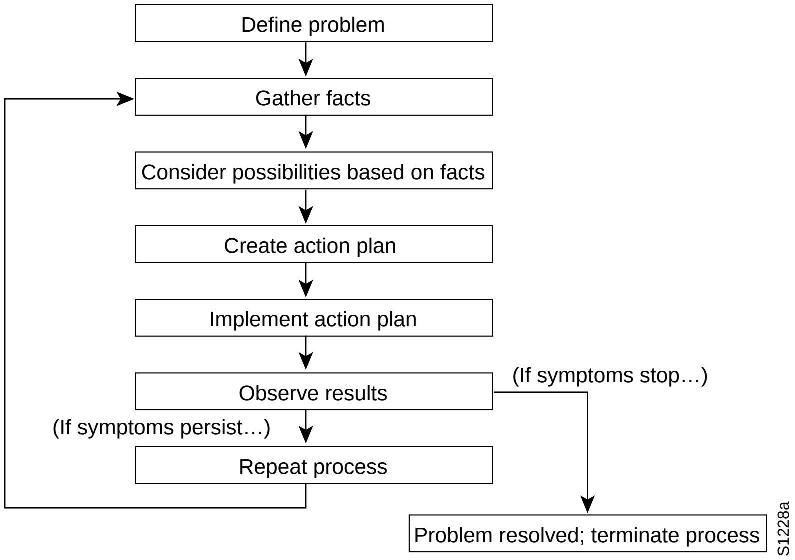
This publication describes how to define symptoms, identify problems, and implement solutions in generic environments. Always apply the specific context in which you are troubleshooting to determine how to detect symptoms and diagnose problems for your specific environment.

General Problem-Solving Model

When troubleshooting a network environment, a systematic approach works best. Define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

Figure 1-1 illustrates the process flow for the general problem-solving model. This process is not a rigid outline for troubleshooting an internetwork. It is a foundation from which you can build a problem-solving process to suit your particular environment.

Figure 1-1 General Problem-Solving Model



The following steps detail the problem-solving process outlined in Figure 1-1:

Step 1 When analyzing a network problem, make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes.

To do this, identify the general symptoms and then ascertain what kinds of problems (causes) could result in these symptoms. For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might be a misconfigured host, bad interface cards, or missing router configuration commands.

Step 2 Gather the facts you need to help isolate possible causes.

Ask questions of affected users, network administrators, managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, output from router diagnostic commands, or software release notes.

Step 3 Consider possible problems based on the facts you gathered. Using the facts you gathered, you can eliminate potential problems from your list.

For example, depending on the data, you might be able to eliminate hardware as a problem, allowing you to focus on software problems. At every opportunity, try to narrow the number of potential problems so that you can create an efficient plan of action.

Step 4 Create an action plan based on the remaining potential problems. Begin with the most likely problem and devise a plan in which only *one* variable is manipulated.

This approach allows you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific change that eliminated the symptom becomes more difficult.

Step 5 Implement the action plan, performing each step carefully while testing to see if the symptom disappears.

Step 6 Whenever you change a variable, be sure to gather results. Generally, you should use the same method of gathering facts that you used in Step 2.

Analyze the results to determine whether the problem has been resolved. If it has, then the process is complete.

Step 7 If the problem has not been resolved, you must create an action plan based on the next most likely problem in your list. Return to Step 4 and reiterate the process until the problem is solved.

Make sure to undo any “fixes” you made in implementing your action plan. Remember that you want to change only one variable at a time.

Note If you exhaust all the common causes and actions (either those outlined in this publication or ones that you have identified for your environment), your last recourse is to contact your Cisco technical support representative.

Preparing for Network Failure

It is always easier to recover from a network failure if you are prepared ahead of time. To see if you are prepared for a network failure, answer the following questions:

1. Do you have an accurate physical and logical map of your internetwork?

   Does your organization or department have an up-to-date internetwork map that outlines the physical location of all of the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, subnetworks, and so forth?

2. Do you have a list of all network protocols implemented in your network?

   For each of the protocols implemented, do you have a list of the network numbers, subnetworks, zones, areas, and so on that are associated with them?

3. Do you know which protocols are being routed?

   For each of these protocols do you have a correct, up-to-date router configuration?

4. Do you know which protocols are being bridged?

   Are there any filters configured in any of these bridges, and do you have a copy of these configurations?

5. Do you know all the points of contact to external networks, including any connections to the Internet?

   For each external network connection, do you know what routing protocol is being used?

6. Do you have an established baseline for your network?

   Has your organization documented normal network behavior and performance so that you can compare current problems with a baseline?

If you can answer *yes* to these questions, you will be able to recover from a failure more quickly and more easily than if you are not prepared.