CHAPTER 1

Troubleshooting Overview

Dependency on network resources has grown tremendously over the past ten years. In today's world, a company's success is highly dependent on its network availability. As a result, companies are increasingly less tolerant of network failures. Therefore, network troubleshooting has become a crucial element to many organizations.

Not only has the dependency for network grown, but the industry also is moving toward increasingly complex environments, involving multiple media types, multiple protocols, and often interconnection to unknown networks. These unknown networks may be defined as a transit network belonging to a Internet service provider (ISP), or a telco that interconnects private networks. The convergence of voice and video into data networks has also added to the complexity and the importance of network reliability.

More complex network environments mean that the potential for connectivity and performance problems in internetworks is high, and the source of problems is often elusive.

Symptoms, Problems, and Solutions

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

This book describes how to define symptoms, identify problems, and implement solutions in generic environments. You should 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 you're troubleshooting a network environment, a systematic approach works best. An unsystematic approach to troubleshooting can result in wasting valuable time and resources, and can sometimes make symptoms even worse. 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 flow 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 properly analyze the problem, 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 include a misconfigured host, bad interface cards, or missing router configuration commands.

Step 2 Gather the facts that 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 that you gathered. Using the facts, you can eliminate some of the potential problems from your list.

Depending on the data, for example, you might be able to eliminate hardware as a problem so that you can 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.

Changing only one variable at a time enables 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 far more difficult and will not help you solve the same problem if it occurs in the future.

Step 5 Implement the action plan, performing each step carefully while testing to see whether 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 (that is, working with the key people affected, in conjunction with utilizing your diagnostic tools).

Step 7 Analyze the results to determine whether the problem has been resolved. If it has, then the process is complete.

Step 8 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, change one variable at a time, and repeat the process until the problem is solved.

Note If you exhaust all the common causes and actions—either those outlined in this book or ones that you have identified for your environment—you should 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. Possibly the most important requirement in any network environment is to have current and accurate information about that network available to the network support personnel at all times. Only with complete information can intelligent decisions be made about network change, and only with complete information can troubleshooting be done as quickly and as easily as possible.

During the process of network troubleshooting, the network is expected to exhibit abnormal behavior. Therefore, it is always a good practice to set up a maintenance time window for troubleshooting to minimize any business impact. Always document any changes being made so that it is easier to back out if troubleshooting has failed to identify the problem within the maintenance window.

To determine whether you are prepared for a network failure, answer the following questions:

- 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 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?

- 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?

- Do you know which protocols are being routed?

  For each routed protocol, do you have correct, up-to-date router configuration?

- Do you know which protocols are being bridged?

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

- 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?

- Do you have an established baseline for your network?

Has your organization documented normal network behavior and performance at different times of the day so that you can compare the current problems with a baseline?

If you can answer yes to all questions, you will be able to recover from a failure more quickly and more easily than if you are not prepared. Lastly, for every problem solved, be sure to document the problems with solutions provided. This way, you will create a problem/answer database that others in your organization can refer to in case similar problems occur later. This will invariably reduce the time to troubleshoot your networks and, consequently, minimize your business impact.