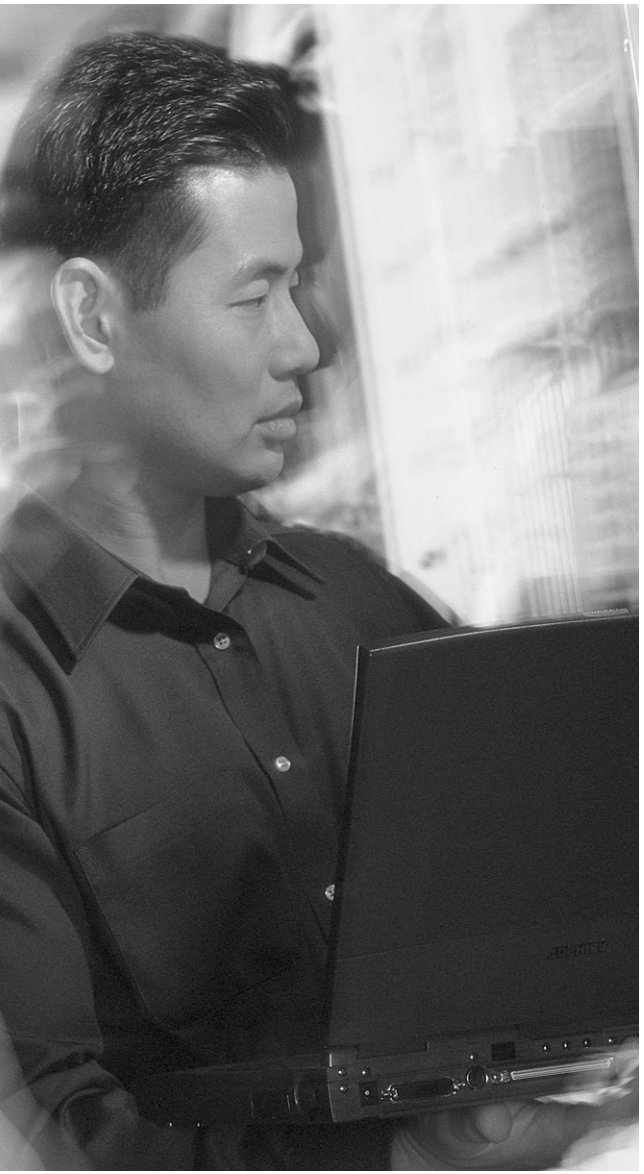


This chapter covers the following subjects:

- The bottom-up troubleshooting approach
- The top-down troubleshooting approach
- The divide-and-conquer troubleshooting approach
- Selecting a troubleshooting approach

CHAPTER 6

Selecting a Troubleshooting Approach

You cannot perform troubleshooting on an ad hoc basis in serious production environments; to effectively solve a problem, you must follow a specific methodology. This chapter presents three main approaches to troubleshooting and describes how to select a suitable troubleshooting approach for the problem at hand. As a troubleshooter, you must take your knowledge and aptitude into account and take the approach you feel is most suitable. With a method to follow, you can solve the problem more quickly and cost effectively than if you approached the problem haphazardly. After you have chosen an approach, do not switch to another one in the midst of the troubleshooting effort. Switching methods often causes confusion, wastes time and effort, and impedes the resolution efforts.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you really need to read this entire chapter. If you already intend to read the entire chapter, you do not need to answer these questions now.

The 10-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 6-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 6-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
"The Bottom-Up Troubleshooting Approach"	2
"The Top-Down Troubleshooting Approach"	3
"The Divide-and-Conquer Troubleshooting Approach"	3
"Selecting a Troubleshooting Approach"	2

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following is an example of a problem that would take place at the network level of the bottom-up approach to troubleshooting?
   a. An interface malfunctions.
   b. A routing loop occurs.
   c. A router heat sink needs to be replaced.
   d. The duplex setting of a port is incorrectly set.

2. If you have exhausted the possibility of the problem occurring in all but the final level of the top-down troubleshooting approach, which layer are you concerned with?
   a. Physical
   b. Data link
   c. Transport
   d. Application

3. Using a divide-and-conquer approach, which layer would you begin with if you isolated the problem to an access list on a router?
   a. Physical
   b. Data link
   c. Network
   d. Transport

4. The power of the Cisco IOS command set encourages which troubleshooting approach?
   a. Bottom-up
   b. Top-down
   c. Divide-and-conquer
   d. Weighted fair

5. During the course of a troubleshooting case, you started checking the physical devices first. Which approach have you taken?

   a. Bottom-up
   b. Top-down
   c. Divide-and-conquer
   d. LLQ (Low Latency)

6. A user has initiated a trouble call, and it seems like a trivial case. Which approach should you most likely take?

   a. Bottom-up
   b. Top-down
   c. Divide-and-conquer
   d. Priority approach

7. Which one of the following is a problem that would occur at the first level of the top-down troubleshooting approach?

   a. The PortFast setting on a port is incorrectly set to off.
   b. The STP state on an interface is incorrectly set to forward.
   c. A jabbering port is identified.
   d. An FTP client application is found to be corrupt.

8. Which of the following provides the guidelines for selecting the best troubleshooting approach?

   a. Apply experience, analyze the symptoms, and solve the problem.
   b. Select a troubleshooting approach and determine the scope of the problem.
   c. Determine the scope of the problem, analyze it using your experience, and solve it.
   d. Determine the scope of the problem, apply experience, and analyze the symptoms.

9. Using the divide-and-conquer troubleshooting approach, you decide to begin troubleshooting a TCP/IP problem at the network layer. You determine that the network layer is working properly. Based on this knowledge, which of the following layers is/are *not* assumed to be working properly?

   a. Physical layer
   b. Data link layer
   c. Transport layer
   d. Application layer

10. Which troubleshooting approach is most appropriate to implement if the problem is located at the network interface?

    a. Bottom-up

    b. Top-down

    c. Divide-and-conquer

    d. Class-based weighted

You can find the answers to the "Do I Know This Already?" quiz in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and 'Q&A' Sections." The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. This includes the "Foundation Topics" and "Foundation Summary" sections, as well as the "Q&A" section.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move to the next chapter.

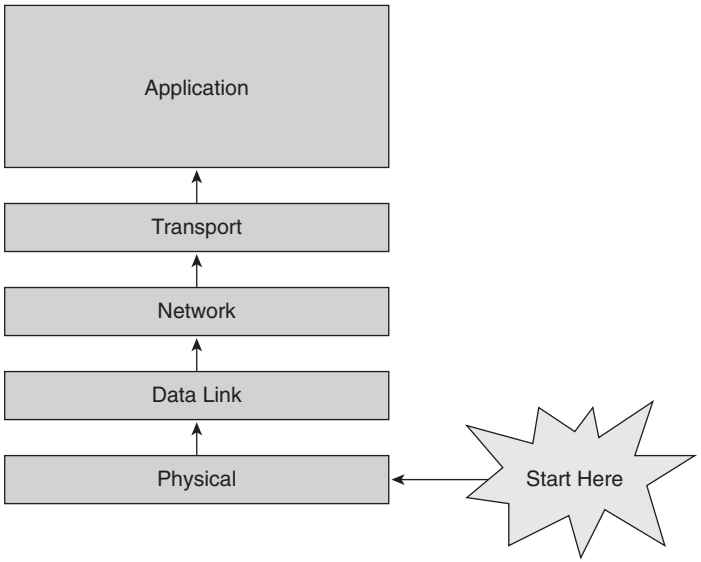
Foundation Topics

The first three sections describe the top-down, bottom-up, and divide-and-conquer approach to troubleshooting based on the OSI layered network model. The final section provides the guidelines on how to select the most effective troubleshooting approach.

The Bottom-Up Troubleshooting Approach

The *bottom-up* approach to troubleshooting a networking problem starts with the physical components of the network and works its way up the layers of the OSI model. If you conclude that all the elements associated to a particular layer are in good working condition, you inspect the elements associated with the next layer up until the cause(s) of the problem is/are identified. Figure 6-1 shows the bottom-up troubleshooting approach.

Figure 6-1 *A Bottom-Up Troubleshooting Approach*



Bottom-up troubleshooting is an effective and efficient approach for situations when the problem is suspected to be physical. Most networking problems reside at the lower levels, so implementing the bottom-up approach often results in effective and perhaps fast results. When faced with a complex troubleshooting case, the bottom-up approach is usually favored. That is because after you ascertain that the elements associated with a particular OSI layer are in good working condition, you can shift your focus on the next layer above, and so on, until you identify the faulty layer.

The downside to the bottom-up approach is that it requires you to check every device, interface, and so on. In other words, regardless of the nature of the problem, the bottom-up approach starts with an exhaustive check of all the elements of each layer, starting with the physical layer, and works its way up. At each layer, selecting the element to start with is somewhat arbitrary because it is up to you as the troubleshooter. One way to avoid having to start troubleshooting from the bottom layer (physical layer) is to test the health of the bottom layers by using the ping or traceroute/tracert tool. A fully successful ping across a link eliminates the possibility of broken hardware (physical layer) or data link layer issues such as mismatch encapsulations or inactive frame relay DLCIs. Ping or traceroute/tracert failure would tell you that problems might exist at the lower layers, requiring investigation.

NOTE When you are testing tools such as ping and traceroute (or tracert on Windows operating systems), you must first ascertain that those applications or the protocols they utilize are supported in the network. In other words, in certain environments, in accordance with management policies, internetworking devices drop or filter packets associated with utilities such as ping or traceroute. In such circumstances, failure of those applications can be misleading or confusing. You can verify whether those applications (or the protocols and the associated application port numbers they utilize) are supported by talking to the administrators or the network engineers. Otherwise, you must inspect the access lists on routers or firewalls.

The Top-Down Troubleshooting Approach

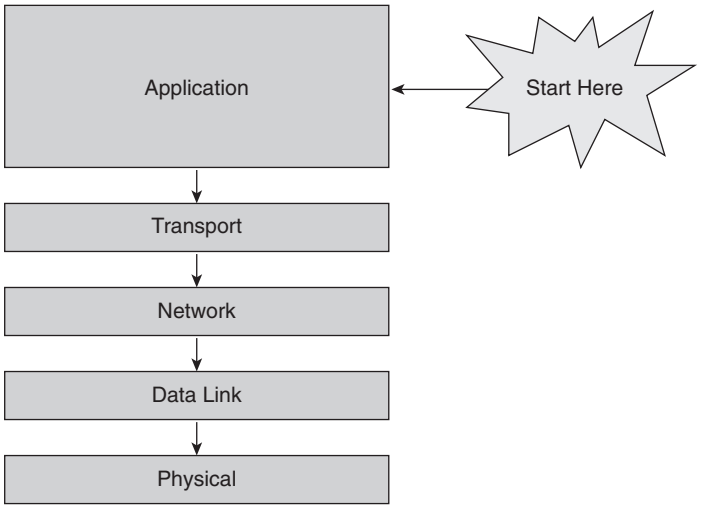
As its name implies, when you apply a *top-down* approach to troubleshooting a networking problem, you start with the user application and work your way down the layers of the OSI model. Figure 6-2 shows the top-down troubleshooting approach. If a layer is *not* in good working condition, you inspect the layer below it. When you know that the current layer is not in working condition and you discover that a lower layer works, you can conclude that the problem is within the layer above the lower working layer. After you have discovered which layer is the lowest layer with problems, you can begin identifying the cause of the problem from within that layer.

You usually choose the top-down approach when you have reason to believe that the problem is most likely at the application or other upper OSI layers. Past experiences, new software installations, changes in user interface, or added security features are common reasons for believing that the reported problems are most likely user, application, or at least upper OSI layer-related. The top-down troubleshooting approach is usually most suitable for problems experienced by one person or only a few people; that is because lower layer (that is, network infrastructure) problems usually affect more than one person.

You usually take the top-down approach for simpler cases. The disadvantage to selecting this approach is that if the problem turns out to be more complex or happens to spring from lower-layer

culprits (physical, data link, or network), you will have wasted time and effort on examining the user applications or upper OSI layer components. Furthermore, if you have internetwork expertise, you might not necessarily have the expertise to diagnose or correct application layer issues. Network engineers often examine the components that fall within their area of responsibility, and if those happen to be in good working condition, the problem is then referred to the workstation, server, or application expert.

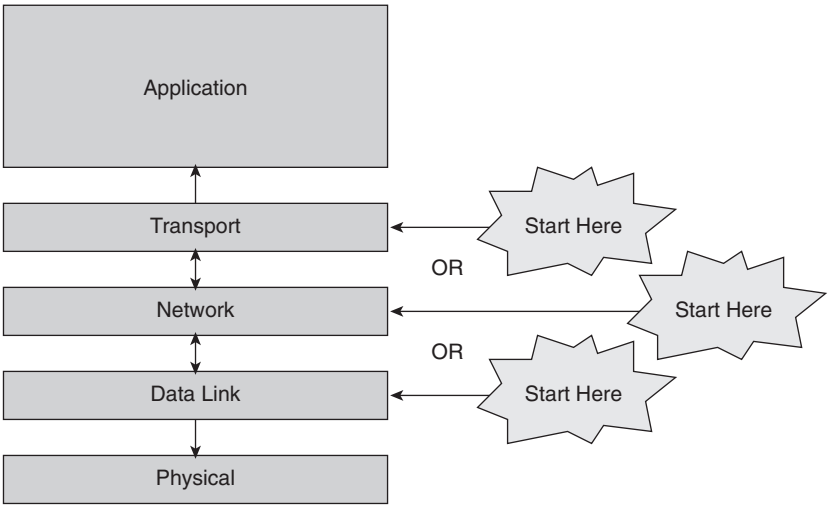
Figure 6-2 *A Top-Down Troubleshooting Approach*



The Divide-and-Conquer Troubleshooting Approach

The *divide-and-conquer* approach to network troubleshooting, unlike its top-down and bottom-up counterparts, does not always commence its investigation at a particular OSI layer. When you apply the divide-and-conquer approach, you select a layer and test its health; based on the observed results, you might go in either direction (up or down) from the starting layer. Figure 6-3 depicts the divide-and-conquer troubleshooting approach. If a layer is in good working condition, you inspect the layer above it. If a layer is not in good working condition, you inspect the layer below it. The layer that you ultimately select as the first targeted layer is the one that is faulty, and the layer below it is in good working condition. The particular layer at which you begin the divide-and-conquer approach is based on your experience level and the symptoms you have gathered about the problem. For example, if a user reports that he can't go to or has some trouble with a particular Web page but has no trouble going to or using other Web pages, you can safely decide that you do not need to begin troubleshooting at the physical, data link, or even the network layer. However, if many users report that they have problems accessing all resources on the Internet, you might start at the network layer and take the next step based on those findings.

Figure 6-3 *A Divide-and-Conquer Troubleshooting Approach*



During the course of divide-and-conquer troubleshooting, if you can verify that a layer is functioning well, you can pretty safely assume that the layers below it are functioning as well. If a layer is not functioning at all or it is working intermittently or erroneously, you must immediately inspect the layer below it (with the exception of the physical layer, which does not have a layer below it). If the layer below the current layer is in good working condition, the culprit resides in the current layer. If the layer below is also malfunctioning, you should gather symptoms of the problem at that layer and work your way down.

Selecting a Troubleshooting Approach

Selecting the most effective troubleshooting approach to solve a network problem allows you to resolve the problem in a quicker, more cost-effective manner. To select an effective troubleshooting approach, you must do the following:

1. Determine the scope of the problem.
2. Apply your experience.
3. Analyze the symptoms.

Determining the scope of the problem means selecting the troubleshooting approach based on the perceived complexity of the problem. A bottom-up approach typically works better for complex problems. A top-down approach is typically best for simpler problems. Using a bottom-up approach for a simple problem might be wasteful and inefficient. Typically when users report symptoms, you should use a top-down approach because of the likelihood that the problem is upper-layer related.

If symptoms come from the network (such as through an SNMP trap, error log, or alarm), using a bottom-up approach will likely be more effective.

Applying your experience means that if you have troubleshot a particular problem (or a similar problem) previously, you might know of a way or a shortcut to expedite the troubleshooting process. If you are less experienced, you likely will implement a bottom-up approach regardless of the circumstances. In contrast, if you are skilled at troubleshooting, you might be able to get a head start by beginning at a different layer using the divide-and-conquer approach.

Analyzing the symptoms allows you to have a better chance of solving a problem if you know more about it. At times, you can immediately correct a problem simply by analyzing the symptoms and swiftly recognizing the culprit.

To make an example for the topic of selecting a troubleshooting approach, assume that you have identified two IP routers in your network that have connectivity but are not exchanging routing information. Before you attempt to solve the problem, select a troubleshooting approach. You have seen similar symptoms previously, which point to a likely protocol issue. Because connectivity exists between the routers, you know that it is not likely a problem at the physical or data link layers. Based on this knowledge and your past experience, you decide to use the divide-and-conquer approach, and you begin testing the TCP/IP-related functions at the network layer. Having chosen to start at the network layer, you decide to ping one router from the router on the other side. If the ping is fully successful, then the problem could be due to restrictive access lists or mismatched settings between the routing protocols at the opposite ends. Therefore, it is apparent that with the divide-and-conquer approach and utilizing your experience, you have arrived near the problem (and hopefully its solution) quickly. Now, again using your knowledge and expertise, you can analyze the symptoms and hopefully identify the culprit.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from that chapter. Although this section does not list every fact from the chapter that will be on your CCNP exam, a well-prepared CCNP candidate should at a minimum know all the details in each "Foundation Summary" before taking the exam.

Table 6-2 *Summary of Troubleshooting Approaches*

Troubleshooting Approach	How It Operates	Cases It Is Suitable For	Advantages/ Disadvantages
Bottom-up	Always starts at the physical layer and works its way up until it finds a faulty layer.	More suited for complex cases.	It is a slow, but solid approach. When the problem is application (or upper layer) related, this approach can take a long time.
Top-down	Always starts at the application layer and works its way down until it finds a faulty layer.	More suitable for simpler problems or those that are suspected to be application/user or upper-layer related.	If the problem turns out to be related to lower layers, you have wasted a lot of time and effort at the upper or application layers.
Divide-and-conquer	Based on the circumstances (reported issues) and your experience, you might decide to start at any layer and work up or down the OSI stack.	Most suitable when you are experienced and the problem has precise symptoms.	It approaches the layer of the culprit faster than the other approaches. You need experience to use this approach effectively.

Q&A

As mentioned in the introduction, you have two choices for review questions. The questions that follow give you a bigger challenge than the exam because they use an open-ended question format. By reviewing now with this more difficult question format, you can exercise your memory better and prove your conceptual and factual knowledge of this chapter. You can find the answers to these questions in Appendix A.

For more practice with exam-like question formats, including questions that use a router simulator and multiple choice format, use the exam engine on the CD.

1. What is the benefit of following a method for troubleshooting?
2. What are the main troubleshooting approaches?
3. Which approach is best for complex cases?
4. Which approach is usually adapted for user-initiated and simple cases?
5. What are the drawbacks of the bottom-up approach?
6. What are the drawbacks of the top-down approach?
7. What are the guidelines for selecting the most effective troubleshooting approach?
8. What does it mean to determine the scope of the problem?
9. What does it mean to apply experience?
10. What is the main benefit of analyzing the symptoms?
11. At which layer of the OSI model does the bottom-up approach to troubleshooting begin?
12. You have isolated a problem to be an encapsulation type mismatch between point-to-point serial interfaces (data link layer). Given this problem, which troubleshooting approach would be the least effective to select?
13. A user has reported that a certain application does not run from his end system. You know that no filters are applied that would prevent the application from working. Running a **traceroute** command verifies that a connection exists between the end system of the user and the application server. Applying a layered approach to troubleshooting, which layer should you troubleshoot next?
14. If you know that a user can access some resources but not others, which layer is the least likely culprit?
15. When you learn that the users cannot browse the World Wide Web, you decide to first check the network layer and, based on your findings, decide what to troubleshoot next. Which approach have you adapted?