Lesson 2: Network Troubleshooting and Maintenance

At a Glance



In the lesson, you will learn the step-by-step methodology followed by many network managers when they troubleshoot their network. Both proactive and reactive approaches to troubleshooting are covered.

What You Will Learn

After completing this lesson, you will be able to do the following:

- Explain what is meant by reactive network troubleshooting and describe a systematic approach to problem solving network situations
- Explain what is meant by a proactive network troubleshooting approach
- Describe several proactive troubleshooting strategies
- Discuss network problem solving tools and techniques, and common networking problems that may arise



Student Notes:

Reactive Network Troubleshooting

Reactive network troubleshooting is a method of keeping the network operational by correcting problems as they occur. The network manager "reacts" to the problem and solves it. Troubleshooting a network problem is the same as trying to analyze or diagnose any other issue that may come up. If your car doesn't start in the morning, you go through a process of discovery. Using the knowledge you have gathered throughout your life about cars, you troubleshoot. You don't immediately call a tow truck and have a mechanic determine what the problem is. Even if you don't know much about cars, you still troubleshoot the simple tasks. You check the gas gauge, make sure you're using the correct key, check the battery for loose connections, etc. You actually go through a systematic approach to solving the problem of what to do to get your car running again.

First, you note that the car does not operate, you use all of the information you know about cars to make an educated guess about what might be wrong. You test out your theories, come to a conclusion, and solve the problem. If you're out of gas, you walk to the gas station. If you can't determine what the problem is, you might call a friend for advice, or read the documentation that comes with the car. If you still can't find and fix the problem, you get a mechanic: the expert. Troubleshooting a network works the same way; you systematically diagnose the problem and try to solve it starting with the simple tasks.

Ideally, if the network is well planned implemented, and maintained, you will not experience problems. Automobile owners who change their oil every 3,000 miles, get tune-ups at scheduled intervals, and pay attention to the gauges in their cars have fewer problems than owners who ignore preventative maintenance and warning signals do. Maintenance includes documentation and this cannot be stressed enough.



The systematic approach you take to fixing your car or that the network manager takes when diagnosing and troubleshooting networks is really what scientists does when experimenting. They follow the Scientific Method. The steps include:

- State the problem
- Research the problem
- Form a hypothesis
- Test the hypothesis
- Draw conclusions and solve the problem

Using the car as an example, the stated problem is that the car won't start. The research is what you have learned over time or the documentation that comes with the car. Suggesting that the automobile is out of gas is the hypotheses. Checking the gas gauge is the test. The conclusion is either the car is out of gas or not. If you reach the conclusion that the car is out of gas, you proceed to solve the problem. If you determine that it is not out of gas, you go on to another hypothesis and test. Network managers follow this same procedure.

State the Problem

If you get complaints that users cannot log on the network and that he or she thinks it is sluggish, you must first determine if there is a problem. Just because there are complaints does not mean there is a network or device problem. It could just as easily be user problems.

When a network user has a deadline in an hour, it is common for a minor problem to be exaggerated. If the user seems excessively excited, try to calm them down and assure them you will do what you can. You must then investigate the problem. If you do determine that there is a problem, you have to prioritize it. A missed deadline by the user may not be the most important problem at the moment.

Research the Problem

First, you do the obvious. Check the connections, are they loose? Next, you try to log on. It's possible the user typed the wrong password in the rush to finish the project. If you don't have any luck, check the configurations on the workstation in case. Is the IP address correct? Is the correct NIC card configured?

You then might proceed to checking all the physical media attached to the malfunctioning device. You ask the user what he or she was doing just before they had their problem. Any clues that will help you determine the root of the problem are valuable. Everything seems fine to you, so you contiue to look for the source of the problem.

Isolate the Problem

If you have a network of 120 workstations on 15 different hubs and you receive 5 telephone calls in as many minutes that people there is a problem, where do you start? The first place is to look at your network diagram—are all of the calls coming from a particular department? Are they all connected to a single hub?

No matter how large your network is, the problems that it will experience fall into two categories—local and systemic. A systemic problem is one that every user on the network experiences. This means that the problem involves a shared resource, device, or program. Before solving a local problem, it must be isolated.

Now you know the extent of the problem and can go on from there. You know from baseline performance data that when the system is running optimally for that time frame that it takes an average of 3 ms (milliseconds or thousandths of a second) to "PING" your POP mail server. You ping a workstation and find that it takes 5ms. You now know that there is a problem. You can now state the problem. The network throughput is low.

You then look at your performance monitoring software—one workstation can't even get it to load for lack of resources, but another has it running. It shows that your servers memory cache is almost full! What might be causing that?



Form a Hypothesis

The fact that there is very little memory available certainly helps to explain why people are having trouble getting onto the network. In addition, processes are competing with each other for very little available memory.

It appears that memory is the issue, so a reasonable hypothesis is that something has made memory unavailable. This can happen a few ways:

- Someone may have removed memory boards from the file server—This is discounted, because the server appears to be untouched, and is still locked in the secure server room. The log also tells you that the computer room door has not been opened since late last night, when the backup media were removed offsite.
- Memory may have become unavailable due to a wiring problem—This may be the case, but the performance manager shows the correct amount of memory; the problem isn't that it is not connected but that it is unavailable.
- Some process is gobbling up the memory—This seems to be a reasonable hypothesis. Memory should be available, and no new software has been installed on the network in at least 2 weeks, certainly nothing that is very memory intensive.

Thus, one hypothesis that makes sense is that a runaway process is using excess memory.

Test the Hypothesis

You move to the system console and run utilities to identify the various processes that are running and where they are running. Everything looks perfectly ordinary, until you get to the second page of the list. There you find that there are 53 PING processes running—no, wait, 54. As you watch for 5 minutes, another ping appears. Where are they running from?

You isolate the PING program and determine that it originated from a workstation in the marketing department. This workstation was assigned to the marketing director who was fired last week.

Draw Conclusions

You conclude that the disgruntled employee set the continuous ping before he or she left the company. You discover a program, apparently written by the fired employee, that runs PING continuously, then, after 5 minutes, regenerates itself to run a second version of PING, and so on, until the system crashes or gets brought to its knees.

The solution is to kill the 55 PINGS running. The system speeds right back up after regaining the memory that PING was using. You print out ping program and remove it to a diskette. You don't want to completely delete it in case the legal department wants to take some action against the marketing manager.

Network Problem Solving

Solving problems on networks has become more complex with the increase in devices, software, and types of services that networks provide. Trying to debug a problem stemming from a video stream was unheard of 10 years ago, and there will likely be applications we are only dreaming about that will be gumming up your network 10 years from now. But no matter what the pieces are, there are some fairly simple rules for trying to solve the problem and form your hypothesis.

Any changes to network software or hardware can create problems. The very first question you should be asking yourself when a problem occurs is "what is new or different?" Some of the places where change might have occurred are with system files, new devices, new device drivers, new accounts, changed privileges, upgraded software, etc.

For example, a new e-mail account is created on the POP server. About an hour later, complaints start pouring in via telephone that there have been no new email messages received by anyone in the company from anyone outside of the company, and they want to know what is happening? Very often, the solution is as simple as having typed an errant character, which make the file with users' email addresses unreadable. By discovering that there is a "f" starting the file name, which shouldn't be there, you are able to correct to problem simply by removing the "f" and then everything's fine.



When troubleshooting, be sure to check only one parameter at a time. If you make multiple changes before checking out the device(s), it becomes difficult to detect the problem.

Often the problem has to do with the installation of new software. A new word processor, for example, may require the resetting of certain of your system-wide parameters to allow for larger buffers and page sizes. While not a problem with most of the programs, older software may be affected.

For example, let's assume that you install new software requiring a certain parameter, called FILEHANDLES; be set to 128 (thus allowing your software to track up to 124 different file names at once.) When installed, you discover that it works fine, but that your spreadsheet program no longer works at all, and crashes during the load on each workstation. You have no idea why this is happening, but strongly suspect it has to do with the new software. You can check the documentation, check the vendor's help desk on the Internet, or check directly with the vendor. You check and discover that the vendor of the new software has encountered this before and can tell you that the spreadsheet software loads the FILEHANDLES parameter into its buffer on startup, but only loads 2 characters. Since FILEHANDLES has a parameter that is now 3 characters long, 128 becomes 12 to the spreadsheet program, which needs a minimum of 64 to function. It crashes for lack of resources. How would you solve this?

There is no easy solution, but there are different approaches you can take. Chances are good that a newer version of the spreadsheet program exists that can handle more than a 2-character parameter. Or you may be able to intercept the loading of the spreadsheet software and use a parameter of 99 for just the duration of the program. Whichever solution you choose, be sure to document it, so that the next person who has to troubleshoot this particular problem can see where the potential problem lies.

Check Your Understanding

- What is network reactive troubleshooting?
- ♦ List steps that may be followed during diagnosing and troubleshooting networks.
- Briefly describe each of the steps from the question above.
- Give an example of reactive network troubleshooting.
- What is a common cause of networking problems?



Proactive Network Troubleshooting

As you know, basic proactive procedures limit reactive network troubleshooting a network manager has perform. You learned about RAID, disk mirroring, redundancy, using management software to set thresholds and alarms, SNMP and other protocol based management, and documentation procedures. All of these are examples of how a network manager can proactively keep the network running smoothly and efficiently.

Network Organizational Planning

Having instituted the above proactive network troubleshooting tactics, you have a network running smoothly. What are some other steps a network manager might take to ensure that the network continues to run smoothly? A plan can be devised that might include the following:

- Scope and timeline for changes/upgrades—Start with missioncritical areas and base recommendations on realistic timelines and resources (budget and technical expertise) considerations.
- **Prioritize**—Which work should come first? What is the schedule for the changes/modifications?
- **Testing plan**—When the changes are implemented they should be done in a controlled environment. Schedule this so that it has the minimum impact on network users.
- **Implementation**—Notify users of the implementation schedule ahead of time so they can plan their work around any disruption this may cause.
- **Retesting**—Once you implement changes, test the network to verify the correct operation of the changes.
- **Documentation**—Again, document all changes/modifications. This will save time and money for continued network improvements.

Security

You already know several important points about security. This section is a quick review of the security issues of which you should be aware.

The goals of security are confidentiality, integrity, and availability. Users expect their data to be confidential. They expect to retrieve untampered data from servers. Users need assurance that unauthorized changes will not occur.

A secure network should prevent "eavesdropping" and unauthorized use. Scrambling and encrypting data as it travels over the physical media will accomplish this task. Unauthorized person access to devices is a priority. In addition, the network should prevent intrusion from unauthorized devices that attempt to alter, steal, or corrupt data as it goes through the network. Prevention and detection mechanisms guard against someone tampering with data. For example, using different passwords for each device limits intrusions. A good security system should also prevent intrusions that make the network unavailable to users because a virus was introduced to the system.

Security measures that help manage network security include the following:

- Wiring closets and equipment physically locked.
- Passwords that are changed frequently.
- A written security policy and is well explained and distributed throughout the organization. The policy must be understood by the individuals who need to know the following:
 - Resources that are secured
 - Procedures implemented
 - Resource availability
- Backups stored in a different physical location from the network.
- Limited dial-up access.



Network Management Systems

Network management systems are also used proactively. Generally speaking, network management systems provide the network manager with the following information, diagnostic tools, and problem solving capabilities:

- A graphical interface that can display physical as well as logical views of the network.
- Industry-standard protocols such as SNMP.
- Automatic "discovery" of new devices.
- A way of storing and retrieving information about network performance.
- Monitoring capabilities.
- Alarm alert functionality.
- Problem solving capabilities.
- Interfaces that allow development of third-part applications.
- Modeling capabilities for cable, hardware, etc.
- Accounting management functionality for tracking network use and billing accounts.

Check Your Understanding

- What is the purpose of network security?
- Give some examples of network security measures a network manager might use.
- Give an example of when it is would be important to ensure network security.
- ♦ What are some proactive network planning practices?
- ♦ Network management systems that provide the network manager with the information, diagnostic tools, and problem solving capabilities. What are some of their features?



Try It Out

Materials Needed:

- Classroom Network
- Optivity software



Monitoring Network Fault Indicators

In this lab, you practice the skills required to identify and locate problems in Ethernet and token ring networks. You will use Optivity applications and options to monitor network and device faults. You will use SNMP notifications and Optivity tools to identify and locate problems.

One of the most important functions in any network is the fault monitoring function.

You will use create intentional errors and faults and use Optivity tools to view the status of classroom network devices and observe how they are affected. In an operational network, the network manager needs to know how to recognize errors.

In this lab activity, your instructor will create problems on different devices, such as turning off the fan on a hub or disconnecting one interface on a router. It will be your challenge to identify the fault using the following techniques.

Part 1: Monitor network faults at hub level using the Alarm panel and the Alarm Manager.

- 1. Start Optivity. Wait for your teacher to set up fault scenario #1.
 - a. In the CCC Folders panel, click on the Hubs folder.
 - b. In the Contents panel, double-click any hub that has changed color.
 - c. In the Attributes panel, click the Alarm tab.
 - d. In the Alarm panel, click the Bell icon to view the alarms.
 - e. Read the details about the notification provided by the Alarm Manager.
 - Record what happens.

- 2. Monitor network faults for a segment or ring using Flat Network View. Wait for your teacher to set up fault scenario # 2
 - a. From the HP OpenView Internetwork View, choose Flatnet View from the Applications menu.
 - b. Click the right mouse button on a ring or segment icon, and choose Diagnostics from the Fault menu.

The Diagnostics window opens for the selected ring or segment.

- List the types of errors present in the space provided below:
- c. Close the Diagnostics window.
- d. Close the Flat Network View.
- 3. Monitor network faults for individual hubs using Segment View. Wait for your teacher to set up fault scenario # 3
 - a. In the CCC Folders panel, click on the LANs folder.
 - b. Select your team's segment or ring and click the Map button.

The Segment View for the selected LAN appears.

c. Select Diagnostics from the Fault menu.

The Diagnostics window opens for the selected ring or segment.

d. Click the right mouse button on a hub and choose Status from the Fault menu.

The Status window opens for the selected hub. This window shows the status of the hub.

- ♦ What is the status of the hub?
- e. Close the Status and Diagnostics windows.
- f. Close the Segment View.



- 4. Monitor network faults for network nodes using NodalView. Wait for your teacher to set up fault scenario # 4
 - a. In the CCC Folders panel, click on the LANs folder.
 - b. Select your team's segment or ring and click the Monitor button.
 - The NodalView for the selected LAN appears.
 - c. Double-click on one of the Errors columns.
 - The NodalView is displayed sorted by nodes with the highest selected error rate at the top of the window.
 - d. Click the right mouse button on the second pop—up menu in the NodalView portion of the window. Select each of the available options to view different MIB groups.
 - e. Click the right mouse button on Properties and choose Net Address to display device IP addresses.
 - f. Pull down the Configuration menu from the menu bar and choose Validate now to obtain current device information. Record the device information in the space provided below.
- 5. Monitor network faults for slots and ports using Expanded View. Wait for your teacher to set up fault scenario # 5.
 - a. In the CCC Folders panel, click on the Hubs folder.
 - b. Click the right mouse button on a hub in the Contents panel and choose Expanded View.
 - The Expanded View for the selected hub appears.
 - c. Click the right mouse button on a port and choose Diagnostics from the Fault menu.
 - The Diagnostics window is displayed for the selected port.
 - d. Close the Diagnostics window.

e. Click the right mouse button on a port or module and choose Status from the Fault menu.

The Status window opens for the selected port or module. This window shows the status of the port. Record the status.

- f. Close the Status window.
- g. Close the Expanded View.
- 6. Monitor router faults using RouterMan. Wait for your teacher to set up fault scenario # 6.
 - a. In the CCC Folders panel, click on the Routers folder.
 - b. In the **Contents** panel, click on a router.
 - c. On the toolbar, click the Monitor button.

The RouterMan window opens.

You can also click the right mouse button on the router icon and choose RouterMan from the menu that is displayed.

d. Click the right mouse button on the Fault icon in the Router section and select Fault Log.

The Fault Log window opens.

- What information is listed at the top of the display?
 Close the Fault Log window.
- e. Click the right mouse button on the IP Fault button in the Protocols section and select Statistics.

The Fault Statistics window opens for each protocol selected.



- f. Note the number of output packets with no routes.
 - A large number of discards for this reason may indicate network configuration problems.
- ♦ How many header errors are shown?
- g. Click the right mouse button on the Ethernet Performance button in the Interface section and select History.
 - The Performance History window opens.
- h. Select the Options button on the toolbar of IP-Performance History.
- What are the seven headings for history data?
- i. Select the Threshold button on the toolbar of RouterMan.
- j. Change a threshold by moving the slide in the Router section.
- k. On the toolbar, select Apply.
- 1. On the toolbar, select the Defaults button. Note all the settings reset to default.
- ♦ What percentage of errors are CRC?
- m. Close RouterMan.
- 7. Use BayStack 28xxx switch Fault Management options. Wait for your teacher to set up fault scenario # 7
 - a. In the CCC Folders panel, click on the Switches folder.
 - b. Click the right mouse button on a BayStack 28xxx switch in the Contents panel and choose Expanded View.
 - c. In the Expanded View window, click the right mouse button on the port you want to reset.
 - d. Choose Reset from the Fault menu.

- e. To display an error log for all ports, choose Error Log from the Expanded View Fault menu.
- f. Select View and LAN architect.

To display an error log for a particular port, click on the port in LAN architect and choose the Diag button from the toolbar.

- ♦ What percentage of errors are CRC?
- g. Close the Diagnostic window for LANarchitect.
- h. Close the LANarchitect window.
- i. In Expanded View for the BayStack 28xxx switch, select the same port as viewed in LANarchitect. Use the right mouse button to select Fault and Diagnostics.
- ♦ What number of errors are CRC?
- j. Close the Expanded View window.

Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
Successful completion of activity	15	
Accurately follows directions	15	
Complete, accurate responses to lab activity questions	20	
Complete summary of experiences included in portfolio	25	
Participation and cooperative teamwork during activity	25	
Other		
TOTAL	100	



Stretch Yourself

Materials Needed:

- Internet connection
- Word processing software



School Help Center - Web Problem Reports

This activity is similar to the help desks designed by major companies as they plan for the support of their netork and customers.

Part 1: Understanding Desk Requirements

Observe several examples of help desks found on the Internet

- 1. The starting point for this activity is to explore the Internet for examples of help desks and the tools that make them successful.
- 2. Try to make a list of the benefits of an efficient help desk to your school or any organization that runs a large network.

Take a look at these web sites for examples of how a Web help site can be implemented:

http://w3.one.net/~alward/

http://help.ptialaska.net/

http://www.island.net/help/

If these sites are unavailable, search for alternates.

Part 2: Understand Tools Needed for a Help Desk.

Determine which tools are needed for a successful help desk and how a help desk can benefit customers of an organization.

- 1. First, decide which model of a help desk you will implement. That will depend on the resources available to you. If your school already has a telephone help desk you may choose to explore how they could set up a web based help desk. Or, you could make it your project to see how the operation of the help desk could be improved. Select one of the following:
 - Telephone and Written Form Model.
 - Internet Form Based Model with Web based help desk.

- 2. Next, come up with a list of necessary components for the creation of your help desk. What things are needed to implement a help desk? What forms, procedures, tools, and resources will you need to create a help desk? Use the Internet and your own research to answer this question.
- 3. Use the Internet to see how other organizations use on-line help forms and telephone support to assist their customers.
- 4. Put your list of help desk resources and tools together in a word processing document for use in the next section.

Part 3: Plan Help Desk Operation, Forms, and Procedures

Plan the operation, forms, and procedures for the establishment of your school help desk.

- 1. Now that you know what you need, start to develop the specific forms, procedures, data, and reference resources for your help desk.
- 2. As you come up with drafts of forms and procedures, discuss them with other students to make this a collaborative effort.
- 3. The results of this activity will be a formal Implementation Plan for your help desk.

Part 4: Operate your Help Desk

Operate a school based help desk.

- 1. Discuss the Implementation Plans other students have prepared and create a single plan for the class.
- 2. Make assignments of responsibility for tasks required to set up your help center.
- 3. Implement the forms and procedures you have designed, and run the help desk for a week or two.
- 4. Review the operation of your help desk and make recommendations that would improve it. Document what you have learned.



Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
Understand the requirements for a help desk and how it benefits the organization that runs it	25	
Understand the tools needed for a successful help desk and the help desk benefits the customers of the organization that runs it.	25	
Plan the operation, forms, and procedures for the establishment of a help desk	25	
Operate a school based help desk.	25	
Other		
TOTAL	100	

Network Wizards

Materials Needed:

- Internet connection
- Classroom networking equipment
- Research materials for safety issues



Network Planning Issues

Listed below are several issues you might have to consider when planning a network. Select one of the choices below and prepare a one-page report that addresses the topic chosen. Share your findings with the rest of your classmates during an informal classroom discussion on network planning.

- 1. When planning networks, designers must consider safety issues. Contact a local building inspector and obtain a list of all permits, licenses, and inspections that must take place when installing networks.
- 2. Connect to http://www.data.com/tutorials/toxic cabling.html and read the article "Cabling: What You Don't Know Can Kill You" by Stephen Saunders.
- 3. Look on the back your computer, hubs, switches, and routers. Notice that there is a label on each one that indicates the amount of current required by that piece of equipment. Check with a local electrician or the vendor that supplied the equipment and ask how they determine if the equipment exceeds the number of amps provided by an outlet. Ask what happens if that limit is exceeded. Ask what they do to prevent the problem.
- 4. Many senior level managers are convinced that their files are too sensitive to be stored on a server. Assuming that the network is not connected to the Internet, develop an argument for such a manager to convince him/her that it is vital to have the files backed up on the server and that the data can be made very secure. As part of your argument, list several ways in which you can secure the data.



Rubric: Suggested Evaluation Criteria and Weightings:

Criteria	%	Your Score
On time delivery of assignment	15	
Complete and accurate summary of findings that demonstrates thorough understanding of topic chosen	25	
Participation in group discussion	30	
Effective communications skills during group discussion	30	
Other		
TOTAL	100	

Unit 4 Summary

Summary

Lesson 2: Networking Troubleshooting and Maintenance

In this unit, you learned how to do the following:

- Explain what reactive network troubleshooting means and describe a systematic approach to problem solving network situations
- Explain what a proactive network troubleshooting approach means
- Describe several proactive troubleshooting strategies
- Discuss network problem solving tools and techniques, and common networking problems that may arise



Review Questions

N	A	V	ΙE
---	---	---	----

Lesson 2: Networking Troubleshooting and Maintenance

Multiple Choice: Select the best answer.

- 1. Which of the following will help you experience fewer network problems?
 - a. Documenting all physical parts of the network, e.g., workstations, ports, RAM, disk capacity, etc
 - b. Developing a visual network diagram
 - c. Backing up the data both fully and incrementally
 - d. Carefully documenting all changes
 - e. All of the above
- 2. Which one of the following is not part of the Scientific Method?
 - a. State the problem
 - b. Research the problem
 - c. Undo the last change
 - d. Test the hypothesis
- 3. Which one of the following is true?
 - a. When troubleshooting, only change one parameter at a time
 - b. When troubleshooting, change all recent systemic changes
 - c. When troubleshooting change all recent local changes
 - d. None of the above

Unit 4 Review Questions

	<i>NAME</i>
4.	You are running a small network and receive telephone calls from almost all users saying they cannot print to any of the network printers. Your problem is probably a:
	a. Systemic problem
	b. Local problem
5.	Which of the following can cause network problems?
	a. New software
	b. Recent change to the network
	c. Broken cable, particularly fiber optic
	d. All of the above
Tr fals	ue/False: Indicate whether each of the following statements is true or se.
1.	The network manager has noticed that the network is slowing down, which clearly indicates there is a problem.
2.	Making-networking changes is one of the most difficult challenges a network manager can face.
3.	A systemic problem involves a shared resource, device, or program.
4.	When you suspect a recent change has caused a network problem reset all changes to save time.
5.	Solving network problems has become more complex with the increase of devices, software, and types of services that networks provide.
6.	There is usually more than one way to fix a problem.
7.	An uninterruptible power supply is only necessary in area where the electricity is know to be flaky.
8.	Diagnostic tools are very helpful in troubleshooting network problems.
9.	A look up time domain reflectometer can be used to measure how far away the problem is.
10.	If all devices operate correctly on an individual basis,

Short Answer:

1. Briefly describe how to go about resolving a local problem.

then they will function properly when interconnected.



ST0025805A

4-67

- 2. When you think you are dealing with a change-based problem, why is it important to only change one parameter at a time?
- 3. Briefly describe each step of the Scientific Method.
- 4. Name three diagnostic tools and describe how they can help the network manager.
- 5. Briefly give advice to a newly hired network manager.

Unit 4 Scoring

Scoring

Criteria	%	Your Score
Check Your Understanding		
Explain what reactive network troubleshooting means and describe a systematic approach to problem solving network situations.	25	
Explain what a proactive network troubleshooting approach means.	25	
Describe several proactive troubleshooting strategies.	25	
Discuss network problem solving tools and techniques, and common networking problems that may arise.	25	
TOTAL	100	
Try It Out:	100	
Stretch Yourself:	100	
Network Wizards:	100	
Review	100	
FINAL TOTAL	500	



ST0025805A

4-69

Resources

Bay Networks, Inc. (1995). *Introduction to Network Management*. Bay Networks, Inc., Billerica, Massachusetts.

Bay Networks, Inc. (1998). Network Management with Optivity for Windows. Bay Networks, Inc., Billerica, Massachusetts.

Craft, Melissa, Poplar, Mark A., Watts, David V., Willis, Will (1999). *Network* +. The Coriolis Group, LLC, Scottsdale, Arizona.

Groth, David. Bergersen, Ben. Catura-Houser, Tim (1999). Network+ Study Guide. Sybex Inc., Alameda, California.

Palmer, Michael J. Ph.D. (1998). *Hands-On Networking Essentials with Projects*. Course Technology, Cambridge, Massachusetts.

Parnell & Null (1999). *Network Administrator's Reference*. Osborne/McGraw-Hill, Berkeley, California.

Sheldon, Tom (1998). LANTIMES Encyclopedia of Networking, Elecetronic Edition. Osborne/McGraw-Hill, Berkeley, California.