EIGHT

Network Tools and Troubleshooting

▲Chapter Syllabus

MCSE 8.1 **Preventing Networking Problems**

MCSE 8.2 **Monitoring Network Operations**

MCSE 8.3 **Troubleshooting Network Problems**

Throughout this book, you learned that a computer network is comprised of many different hardware and software components, nearly all of which are created by different manufacturers.

Components work well together despite their various origins, because manufacturers adhere to internationally recognized industry standards for data and telecommunications.

Network components are typically purchased separately. That is, a network administrator may decide that a fiber optics backbone is the best choice for the network and twisted pair for clients connections. Likewise, a router may be used to organize smaller LANs into a large LAN; A repeater can be used to boost network signals and extend the technical length of a network topology.

Together, selected components form a network. However well the network functions, the network administrator must monitor network operations regularly for signs of network problems.

There are various kinds of network problems that can occur, including but not limited to breachs of security and temporary or permanent degradation of network response time. Some are easy to detect and fix while others require good detective work. You'll learn about techniques for monitoring the network, planning for trouble, and how to handle network problems when they arise.

MCSE 8.1 Preventing Networking Problems

The old saying, that an ounce of prevention is better than a cure, holds true for computer networks. Although all the planning in the world won't guarantee that the network will keep running forever. A good plan will minimize the impact that a network failure will have on the organization's ability to operate.

It is the responsibility of the network administrator to develop good administrative planning for the network, which will reduce the opportunity for mistakes. The plan must consider network security, standardization procedures, good documentation of all procedures and network topology, backups of network resources, and regular maintenance and upgrading of network components.

The Network Security Plan

Network security involves more than preventing an intruder from accessing network resources. In fact, there are very few accounts of such attacks when compared with the number of people who use networks daily (Figure 8–1).

Of greater concern is the likelihood that someone who has legal access to the network will do something inadvertently to halt network operations such as deleting the client database. This includes network administrators whose mistakes because of access privileges can be irrecoverable.

The best way to reduce the chance of these errors from occurring is to establish and strictly enforce access restrictions. Access restrictions limit network resources that a person can access and specifies how the person can use those resources.

One of the most exposed and most used network-resources is a file server. A file server contains data files that can be shared among network users. Typically, everyone on the network will be able to access the file server. However, each person should be restricted to those directories relevant to their job. Furthermore, it may be advisable to limit a person to a particular file(s) within the directory and grant that person readonly or read/write access to those files as needed.

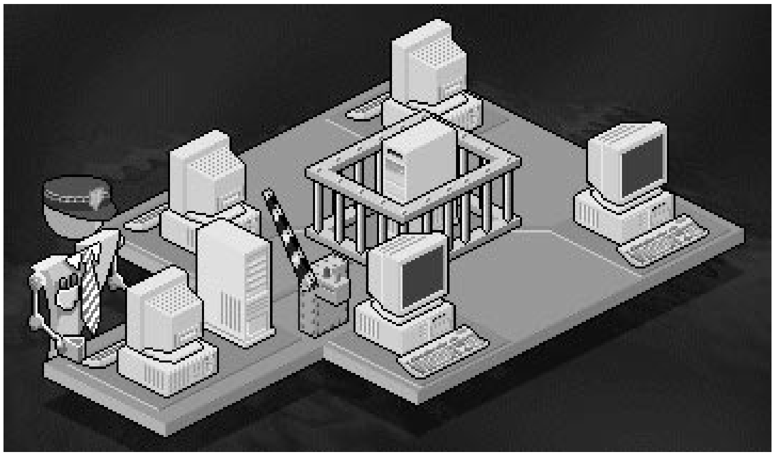

Figure 8–1. *Enforcing the network security policy is the first line of defense against an attack on the network.*

A person who has read-access can view information stored in the file, but is not able to modify or delete the information. Write-access gives a person the ability to change information and inadvertently corrupt the data in the file.

While network software such as Windows NT provides the utilities to limit access to network resources, it is up to the network administrator to institute the access restrictions described in the network plan.

Imposing access restrictions on network users can meet with resistance, especially when some see these limitations as an impairment to a smooth running organization. A network administrator must be careful to strike a balance between network protection and the need to use network resource as a tool for doing business.

A good approach to take is to identify the owner of the network resource, then let the owner decide which users are granted access to the resource. The owner is probably the best person to weigh the business needs against the need for protection.

For example, the owner of a file is in the position to identify which user should see the information stored in the file and whether or not that person has a need to modify the information.

Likewise, the network administrator takes ownership of network resources such as printers, printer servers, and fax/modem servers. In a large organization, the network administrator may want to delegate management of a network resource to an assistant. Only the designee and the network administrator will have access to modify the resource.

Network administrators that adhere to the ownership method of granting access rights typically institute a sign-off procedure whenever anyone requests access to a network resource. In addition to the normal security clearance required to receive a network login, permission must be obtained from the owner of the network resource before access is granted.

This policy gives the resource owner sign-off control over the resource, although physical control to the resource remains with the network administrator. That is, the network administrator can ignore the sign-off policy and grant access to any user to any network resource.

Standardized Procedures and Good Documentation

A computer network can be a hodgepodge of hardware and software (Figure 8–2). Although components work well together, each manufacturer has its own way to connect to the network.

This becomes evident when routers from different manufacturers are used on the same network or each of smaller LANs in the organization use different network operating systems.

These variations make any network more complicated than necessary, because the network administrator must learn how to configure and maintain several different network devices that have the same functionality, such as routers made by different manufacturers. If you have 3 different routers made by 3 different manufacturers then you will probably have 3 extremely different configuration procedures which might involve reading 3 different manuals all to accomplish one function.

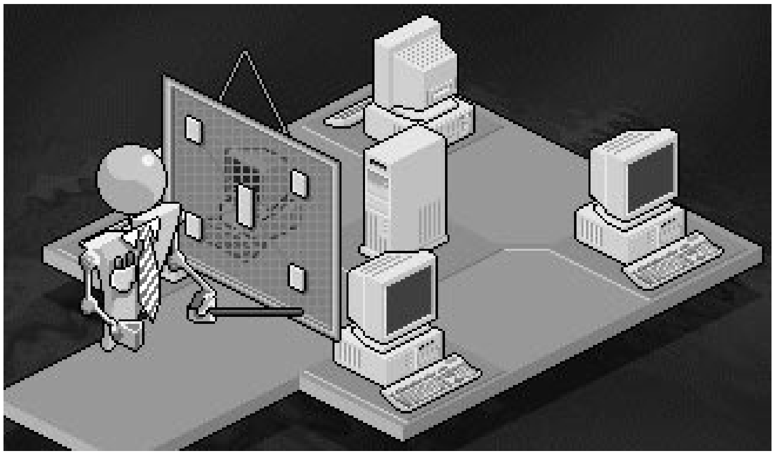

Figure 8–2. *Network documentation should include the location of all network components.*

A better approach is to standardize network components. For example, find the best network operating system for the organization's needs, then plan to use it on all the networks when possible. Likewise, use a router from the same manufacturer when possible.

Standardizing components before the network is installed makes supporting network operations more efficient. Each component has setup and maintenance procedures that can be incorporated into a handbook to help network technicians keep the network running.

Each procedure should be a step-by-step guide that walks a technician through the process. Most of these procedures can be copied from the manufacturer's documentation. However, the network administrator will need to include settings, called configurations, that are relative to the organization, such as locations of network resources.

The combination of standard components and standard procedures simplifies network administration and reduces the operating cost of network support. This becomes evident when an organization loses a network technician.

The network administrator can use the procedure handbook to train another staff person to handle routine tasks until an experienced replacement can be found. In many cases, the staff person permanently fills the position, because 80 percent of what the technician needs to know about the network is found in the procedural handbook. The network administrator can supplement the missing 20 percent.

The procedure handbook should contain more than procedures. It should contain the physical location of network components in the organization. Some network administrators include floor plans of each floor, which identify all the departments that occupy the location, desks, jack locations, type of wiring, and desk numbers. Desk numbers are referenced when a trouble call is received from a user.

Also found in the handbook should be the names and telephone numbers of secondary support staff. These are the people, sometimes manufacturer's reps, who can help the technician resolve problems that are not contained in the procedural handbook along with device configuration information, make and model number.

Backups

A network plan must consider contingencies. What will you do if something catastrophic occurs? All of us hope network operation will continue to run smoothly, but there will be a time when a critical component of the network breaks down and disables the network.

You can't prevent hardware failures, but you can develop a plan to minimize the network downtime when hardware failures occur. The best approach is to have backups available that can immediately take over for the failed component. Backups (Figure 8–3) typically refer to copies of software and data stored on network servers that should be copied to tape or CD regularly, as described in Chapter 7.

Backups can also refer to having duplicate hardware available on site. It is not uncommon for an organization to have drop cables, connectors, hard disk, modems, network adapter cards, and even ready-to-run servers available to go online at a moment's notice. Any network component that could fail and interrupt business should be replicated on site.

For example, what happens if a database server crashes? If there is a back up server on site you can immediately restore the data from the tape backups and very quickly and efficiently replace the crashed server with a working one. Once the replacement server goes online, technicians can concentrate on troubleshooting and repairing the failed server.

Having a sufficient backup plan is costly and may be beyond the economical reality for smaller organizations. For example, it probably isn't economical for an organization that has one server to have a backup server, although software and data files stored on the server should be backed up on tape.

The network administrator should conduct a risk analysis to determine how much of a backup plan is needed by the organization. A risk analysis is a review of network operations and components to assess the chances of failure and the economical cost of those failures. Risk analysis must consider these factors:

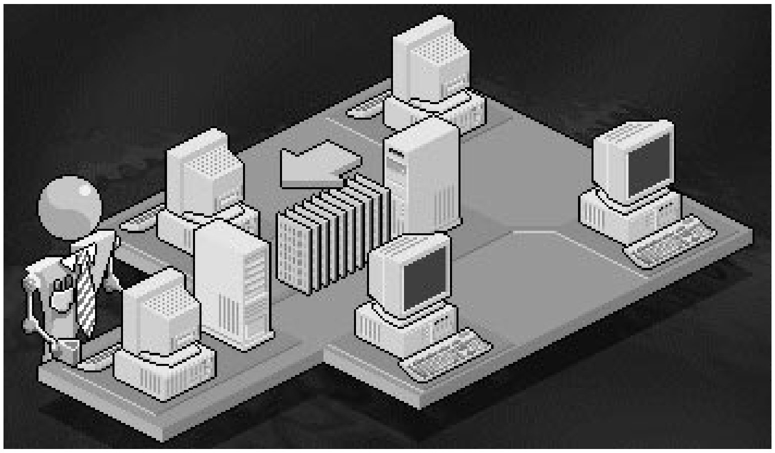

Figure 8–3. *Backup files can be restored whenever files become corrupted, therefore minimizing the network downtime.*

- How much would the organization lose if a particular component (i.e., server) became disabled?
  The network administrator must answer this question in the context of each component and the estimated length of time the network would be unavailable. For example, a five-hour malfunction of the network segment that supports the accounts payable department might have little effect on the organization. In contrast, the organization would be deeply hurt if the telephone sales department's segment were offline for even an hour.
- How soon can the malfunctioned component be replaced?
  An assessment must be made to determine how quickly replacement parts can arrive at the site if they are not stored on the premises. As a general rule, the longer to delivery time, the more the network administrator should consider having a replacement part on hand at all times.
- What is the failure rate of network components?
  No one can predict when a component will break down, but component manufacturers typically have specifications citing their experiences. This is called the component failure rate and is sometimes identified as the number of hours of operation before a failure occurs. The network administrator should consult with the component manufacturer to determine the failure rate of each component. Once known, the network administrator can estimate the time frame when the network component is likely to fail.
- Is it economical for the organization to stock replacement components?
  This isn't an easy question to answer. For example, an organization may invest $20,000 for a backup server that wouldn't be used for years. Yet, the server could be disabled in six months and the backup server becomes a lifesaver. Here's an approach to take when answering this question.

  First, determine how much money the organization would lose per hour if a component in the network fails. For example, practically no economic loss would occurs if a client's drop cable or connectors malfunctions. However, a drop cable connecting a router to a server could have an economical effect on the organization.

  Next, determine how soon a replacement component can be delivered. If your supplier can deliver the component within the hour, then it is unlikely you'll need to have a supply on hand. However, the longer the delivery time, the more money your organization could be losing.

  Finally, determine if the cost of having the replacement component in stock is less than the money the organization would lose. If so, then you should seriously consider stocking those components.

Keep track of replacement components. Make sure they are clearly labeled and store them in an equipment closet in an orderly manner. Make sure boxes containing components are properly labeled and contain all necessary documentation so that a technician can find them in an emergency. Also be sure components are inventoried at least once a month to determine if components should be reordered.

Maintenance and Upgrades

Network planning must include scheduled maintenance of hardware. Maintenance is probably the most overlooked factor involved with keeping a network operational, because the impact of maintaining a network isn't obvious.

For example, removing the buildup of dust inside a router doesn't make the router perform any better than if the dust was allowed to accumulate. However, dust can increase the operating temperature of the router by reducing the cooling area of circuits inside the route. Eventually, the increased heat will take its toll on the router.

A good maintenance schedule will include:

- Making sure all network cable connects are tight. A loose cable can cause intermittent network outage for a client—and a headache when troubleshooting the network.
- Removing dust from the inside of all electronic network components. This includes network components and clients.
- Comparing the in-service time of components with the failure rate of the component. The in-service time is the length of time a component has been connected to the network. You can expect a problem with the component to occur if the in-service time is close to the fail rate.
- Examining the network response time for various network segments. If response time is slowly becoming unacceptable, then plan to reorganize the segment.
- Testing all components to make sure they work correctly. Some network components such as printers or fax-modems may be underutilized by clients and may not be operational. For example, a network may have ten fax-modems, but only four of them are used frequently.

The network administrator should create a network maintenance log that contains the maintenance schedule of network devices, maintenance procedures, and information on when those procedures were performed and who performed them.

You can consider the maintenance log like a patient's hospital chart. The log should detail the status of the component during the maintenance check. This can be compared to previous status reports to determine if a trend is occurring, such as a steady decrease in network response time. The trend frequently points to future troubles that can be avoided before the problem affects network operations.

Maintenance procedures are typically supplied by the component manufacturer and are usually found with the owner's documentation that is supplied with the equipment. Follow these procedures carefully. Not only do they support any warrantee claims you might make to the manufacturer, but they also prevent the device from failing prematurely.

In addition to developing a good maintenance plan, the network administrator should make sure all network devices are upgraded, as required by the equipment or software manufacturer. An upgrade is the replacement of part of the component (Figure 8–4).

Some organizations are skeptical about manufacturer-recommended upgrades, since many of these require the company to pay for the upgrade. Is an upgrade a ploy by manufacturers to make more money or will the upgrade provide more service?

This isn't an easy question to answer. However, upgrades are commonly issued to fix bugs in the product. It is always wise to discuss the difference between the upgrade and your current product with the product's manufacturer before installing the upgrade. This provides a rational for upgrading your network.

A word of caution. An upgrade can cause problems with the network operation. It is mandatory that you backup components before you perform

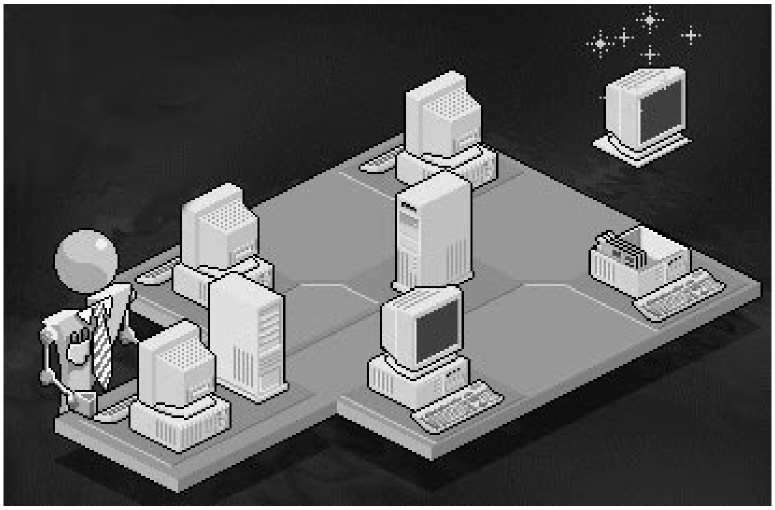

Figure 8–4. *The network administrator must make sure upgrades to network hardware and software are made in a timely fashion.*

the upgrade. All upgrades should be installed and tested on a Friday night. This gives you the weekend to fix any collateral problems that might arise from installing the upgrade.

MCSE 8.2 Monitoring Network Operations

A good network-operating plan needs to be augmented by consistent monitoring of information throughout the network. Monitoring network operations gives the network administrator an insight into how well the network design meets the needs of the organization.

The need for network services changes slowly as network usage grows. As you learned throughout this book, these gradual changes tend to exceed the original design, which can cause degradation of performance.

Monitoring the network regularly enables the network administrator to see clues of forthcoming difficulties so that preemptive action can be taken before users notice a drop in network services.

Many network operating systems provide monitoring software that adheres to the ISO's five network management categories. These are: accounting management; fault management; performance management; security management; and configuration management.

Accounting management monitoring is a utility that tracks the usage of network facilities. For example, the network operating system makes note each time a user logs into the network and uses a network resource.

Fault management monitoring tracks the workings of network components. The monitor then detects components that failed to work and reports problems to the network administrator.

Performance management monitoring tracks the flow of data throughout the network. Typically, the performance management monitor receives and counts all the data packets that flow through the network.

Security management monitoring involves making sure users have proper access to network resources. Configuration management monitoring is used to set the parameters of the network operating system and of network components.

Network performance is the ability of the network to transmit data at a reliable and consistent speed. As demand for network resources increase, traffic across the network also increases and the response time of the network gradually decreases.

It is the job of the network administrator to identify and resolve network performance problems. The network administrator's initial step is to create a baseline measurement of performance when then network is running smoothly. This defines the normal network performance called a **base-**

line. Baseline measurements should be taken using tools like Windows NT Performance Monitor after a network becomes fully operational.

On a regular schedule such as the first Friday of every month from 10 a.m. to 2 p.m., the network administrator should take the same measurements of the network and compare the results to the baseline measurements. Over time, this comparison shows a trend in the network performance.

If the trend indicates degradation in network performance, then the network administrator must identify the cause of the problem, which is called a **bottleneck**. Any network component can be a bottleneck if it impedes the flow of data across the network.

A bottleneck does not necessarily mean a network component has malfunctioned. It could simple mean network traffic patterns have changed or network upgrades have increased transmission speed beyond the capability of the device that is causing the bottleneck.

Network performance measurements compared with a baseline indicate if a network performance problem exists. The next question the network administrator must answer is which component is causing the bottleneck.

Here are the more common sources of network bottlenecks:

CPU speed of a server
Available memory of a server
Network interface cards in a server
A server's disk controller cards.
Routers
Gateways

Tracking Down Bottleneck

It is common that complaint about network performance will stem from users who are connected to the same network segment. Therefore, it is important for the network administrator to gather as much information from persons who complains as possible. For example, you'll need to know the person's location, telephone number, computer name, and a detailed description of why the person believes there is a network problem. Ask detailed question such as "has this ever happened before? "What time did you first notice it?" and "have you moved your computer recently?" Reviewing the locations of all the complaints will tell you which network segment is experiencing a performance problem.

Next, you'll need to review the network maintenance log to determine if any network component has been recently changed. If so, then that component is your first suspect. If not, then you must identify all the network components that are connected to the segment.

Measure network traffic in the segment using a protocol analyzer. This provides you with a real-time analysis of data flow and a snapshot of network components on the segment. You can compare the results of this analysis with baseline measurements to isolate the bottleneck.

If network components seem unlikely suspects based on the results of the protocol analyzer test, then suspect the cabling. Check cables to the NIC card and to the jack first. You can identify cable problems by using A Time-Domain Reflectometer (TDR) or a network analyzer. Compare the results of the cable test with the baseline measurements to determine if the cabling is at fault. If it is, then the cabling needs to be replaced.

Network components and the cabling may not be the source of the problem. In that case, determine if a new application is running on a client or server. A new application could be transmitting an unusual amount of data traffic such as stock ticker application that updates many clients on a segment several times a minute.

Also, don't overlook the possibility that a few users are playing games over the network. A case in point occurred in a major international Wall Street firm. Traders were playing air combat against the sales staff who was located in another building. The entire trading floor network slowed to a snails pace.

If the problem is caused by an application, you can ask users to curtail use of the application, ask the software developer to modify the application, or plan to increase the size of the network to accommodate the application.

However, if software isn't causing the problem, then it might be time to redesign the network. The organization has likely outgrown the original network design as the last resort.

Techniques for Reading a Monitor

Network monitors collect information and count certain activities on the network and relate them to the time the activity occurred. This information can then be displayed in various ways to help the network administrator analyze network operations.

For example, a performance monitor can display the number of data packets traveling across the network per hour as a graph. This enables the network administrator to determine the maximum volume of traffic over the network.

Once a network is installed and has stabilized, the network administrator should run all the monitors to determine a baseline for the network. A baseline consists of statistics that represents acceptable performance and must be stored for future reference (Figure 8–5). Many network-monitoring utilities provide a facility to save network statistics.

Each time the network is measured, the network administrator should compare the results of monitoring to the baseline. This helps to determine if current network activities conform to acceptable levels.

An acceptable level is subjective within an acceptable tolerance range. For example, many users won't complain if there is a couple of seconds of delay in the network response. However, a volume of complaints can be expected if there is a ten second response time.

The network administrator should track the date and time of all user complaints and associate them with network statistics at that moment. This provides the network administrator with an unacceptable level.

Network monitors can be used to forecast trouble before it arises so long as the network administrator establishes a baseline and an unacceptable line. As statistics move closer to the unacceptable line, the network administrator can anticipate trouble and take measures to avoid the problem and reduce the progression toward the unacceptable line.

Windows NT Server and Monitors

Windows NT Server contains a utility called the **Performance Monitor** that is ideal for tracking network operations. The Performance Monitor offers two methods of counting network events; realtime and recorded time. If the events

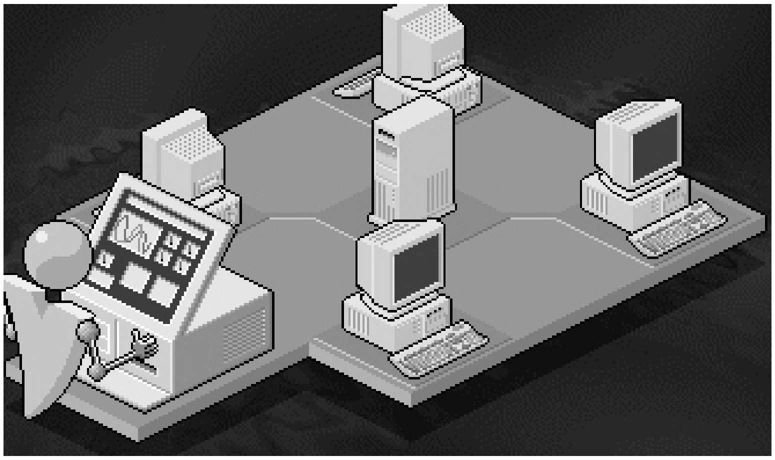

Figure 8–5. *Develop a baseline of key network parameters once the network is stabilized.*

are recorded and counted as they occur, it's called **realtime**. If the events are logged to a file and then analized at a later date, it's called **recorded time**.

From the data captured by the Performance Monitor, the Network Administrator will be able to spot bottlenecks in the network and determine the impact that modifications have on network operations.

Each event, called a **counter**, can be displayed on the screen, saved to a log, or printed in a report. Also, the network administrator can set up a threshold value for each counter. If the value of the counter falls above or below the thresholds then the Performance Monitor sounds an alarm that alerts the network administrator to the problem.

Another useful monitor you'll find with the Windows NT Server is the Network Monitor, which tracks data packets flowing over the network. The Network Monitor copies data packets into a log. Information in the log can be filtered by network address, data packet type, or by any pattern of characters.

MCSE 8.3 Troubleshooting Network Problems

The most important role of a network administrator is to be able to quickly respond to disruptions in network operations. When a network malfunction occurs, the network administrator has two objectives; to locate the trouble and correct the problem.

Typically, a malfunctioning component can be corrected quickly if the network administrator implemented a good network plan, as is discussed earlier in this chapter.

However, locating the troubled component is an ardent task, since there could be hundreds of network connects in a large network, thousands of feet of cable, and many routers, repeaters, and other line devices. Anyone of them could be the culprit and it is the job of the network administrator to track down the problem within the shortest time frame.

In this section, we'll explore some of the proven techniques that are used to troubleshoot a network. Following these methods will reduce troubleshooting to a minimum.

Organize for Fast Reaction to Complaints

The network operations support team must establish a help telephone number that can be called when a user experiences network trouble. The help line needs to be supported by a technician whenever people are working. This typically includes extended business hours and weekends.

Procedures should be created by the network administrator to guide technicians through the process of addressing the user's network problems.

Procedures provide the most efficient way to approach a network problem. Here's what needs to be included in these procedures:

•. Identify the caller by login ID and client location. This information helps to pinpoint the network address that is experiencing a problem.

•. Identify the problem. The technician needs to be able to interpret the user's complaint into technical terms.

•. Replicate the problem if possible. The technician should try to connect to the remote client using software such as Timbuktu, which lets the technician take over a client without having to visit the client's site.

•. Determine the severity of the problem. The technician needs to determine how the network malfunction affects the business by questioning the caller.

•. Set the priority of the call. Compare the severity of the problems with other outstanding network problems. The most severe problem must be addressed before all others. This is called triage.

Research the Problem

A complaint call reveals the experience encountered by the user. This alone is not sufficient to address the user's network problem. Instead, information gathered from the call provides the network support technician a starting point from which to further explore the situation.

The caller typically makes a passionate plea for help that sometimes is tainted with accusations and condemnation of technicians that run network operations. Somewhere in the midst of the call, the caller gives the network support technician clues, some of which are pertinent to the problem and others that are not related.

It is the job of the network support technician to sort through the information to identify clues that will be helpful in tracking down and fixing the problem. Once the information is elicited from the caller, the network support technician must systematically research the information. Here are a few factors that research should address:

- Has the caller complained about a network problem recently?
  Each call should be recorded in a log, where the nature of the problem is listed along with details of the steps used to attempt to fix the problem. Both successful and unsuccessful steps should be entered into the log. If the caller experienced previous problems, then there is a high probability that the problem wasn't fixed and could be an intermittent problem or the remedy could have caused another problem. An intermittent problem is one that occurs irregularly and is difficult to repli-

cate. The research provided can narrow the scope of the technician's tests and possible solutions.

- Have other callers complained about the same network problem recently?
  A network malfunction typically affects more than one user. The call log can be searched to identify recent callers that have recorded similar problems. This information can help to narrow the network fault to a common device, such as a router. A router, as discussed previously in the book, is the network device that directly connects clients on different networks. Drop lines from clients are connected to a hub, which is connected to another router on the network.
- What network events occurred around the time the user experienced the problem?
  A change in the network or a specific sequence of events could be the cause of a network problem. For example, a new repeater that has been installed on the network or if a router's router table was reconfigured are changes that may or may not have influenced network failure. Likewise, network activities that occur in a certain sequence could cause an intermittent network problem. The network support technician must examine call logs, maintenance records, and, in the case of an intermittent problem, network monitors to determine network changes and patterns. The objective is to collect information. The network support technician who must diagnose and fix the problem will determine whether or not the information has a bearing on the problem.
- Has any network user reported a similar problem in the past?
  Rarely is a network problem unique. Many problems have occurred previously—although not necessarily recently—such as a malfunctioning router or a loose cable connection. Caller, repair, and maintenance records should be reviewed to identify previous occurrence and to learn steps used to solve the problem.

Isolate the Problem

After a complaint is received and researched by a network support technician, the source of the problem must be identified. This is called isolating the problem. Network complaints arise from four general areas of network operations: software, hardware, user-training, or network design.

Software and hardware problems can be located at either the client or the network level. For example, the client requires client-side network software configured to use the proper protocols; a valid network ID and password; a network interface card; and a proper type of cable connection to the router. The network contains the network operating system; routers; repeaters, bridges, fax/modems, printers, servers, related cabling, and other network devices.

Analyzing the information that is known about the problem can help isolate a network problem. Here is a procedure (Figure 8–6) that can help to track down the troubled network component.

- Is the problem located on the client or the network?
  When more than one caller complains about the same problem, the trouble is likely located on the network side rather than the client. An exception to this rule is if new client-side software was recently installed, then the network support technician should suspect a configuration problem with the software installation as the culprit. However, if there is only one reported incident, then the client side is a good place to begin the investigation.
- If the client side is suspected, is the client's address active on the network?
  Network operating systems provide a utility to test if a network address is active. This is called *pinging* the address. If the address is not active, then the network support technician should suspect problems with the client's network interface card, the drop cable connection, the router port to which the client is connected, and possibly the router table. If the address is active, then problems with network software on the client side should be suspected.
- If the network side is suspected, is there commonality among clients who report problems?

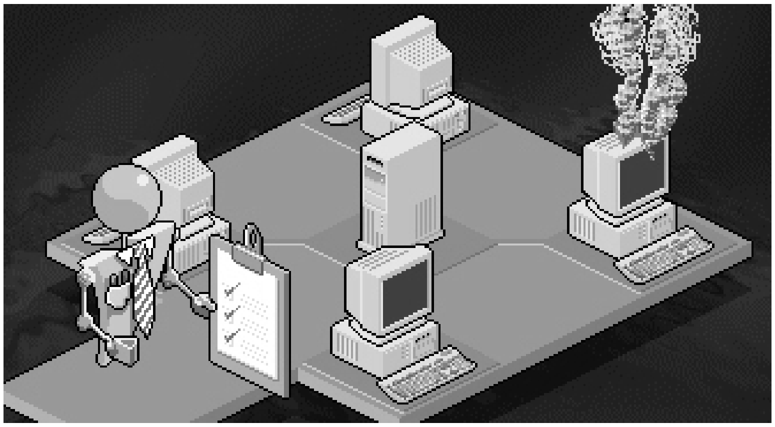

Figure 8–6. *Always follow a procedure for troubleshooting a network problem.*

Typically, there is something in common with users that complain about the same problem at the same time. For example, all of them might be on the same network segment serviced by the same router or other network device. Likewise, they might use the same network printer and be unable to print documents. Refer to the network layout to trace clients to common devices, then examine shared devices, beginning with the first device common to clients.

- If the client side appears to be operating properly, is the user properly trained?

  The network support technician needs to visit the user or remotely connect to the user's computer and ask the user to repeat the steps that lead up to the problem. It will become apparent if the user makes an error. For example, a network operating system may require a user to enter the proper case for a password. The user may have inadvertently activated the cap lock on their keyboard, then complained that they can't log onto the network.
- If the network side appears to be operating properly, is the design of the network causing the problem?

  An organization can easily grow beyond the initial design of the network. This growth can lead to all kinds of problems. For example, users would complain about poor network response time or of intermittent problems on the network.

Troubleshooting Network Devices

Once the network support technician has isolated the problem to one or more network devices, each device must be examined and tested to determine if it is at fault. Manufacturers of many network devices provide guides for troubleshooting their devices. They list step by step procedures which should be followed, starting with the most common problems down to the less common. These include routers, bridges, repeaters, and gateways.

As a general rule, try the simplest solution first to fix the problem. Let's assume one client cannot communicate with the network and you've pinged the address to find the address is not active. Examine the cable connection before replacing the network adapter card or conducting more sophisticated tests on the network.

Network support technicians should use the most efficient technique for locating a malfunctioning network device. Sometimes this involves swapping a device known to work with one that is suspected of causing the problem. This technique is at times faster than using sophisticated test equipment to locate the problem.

However, network components such as the backbone cable cannot be easily replaced and therefore test equipment is required to determine if the component is working properly. There are a number of common test equipments used to track down network problems. These include Time-Domain Reflectometers (TDRs); oscilloscopes; a digital voltmeter (DVM); protocol analyzers; and a cable tester.

TDR (Figure 8–7) is a tool used to test cables. It does this by sending a sonar signal across a network cable, then analyzes the strength of the returned signal to determine the condition of the cable.

Typically, a TDR is used with an oscilloscope to display the voltage of the pulse. The oscilloscope shows voltage over time in a graphical form on the oscilloscope screen. This enables the network support technician to see the decay of the signal as the signal is reflected back to the TDR. The TDR and the oscilloscope are mainly used during the installation of network cables, although they can be a necessary tool when identifing a problem with an existing cable.

A **DVM** is another tool commonly used by a network support technician to determine the flow of current through a cable and other network devices. The DVM measures both the voltage of the signal and the resistance of a device. Think of voltage as the force of the signal over the cable and resistance as the force pushing against the signal by the cable.

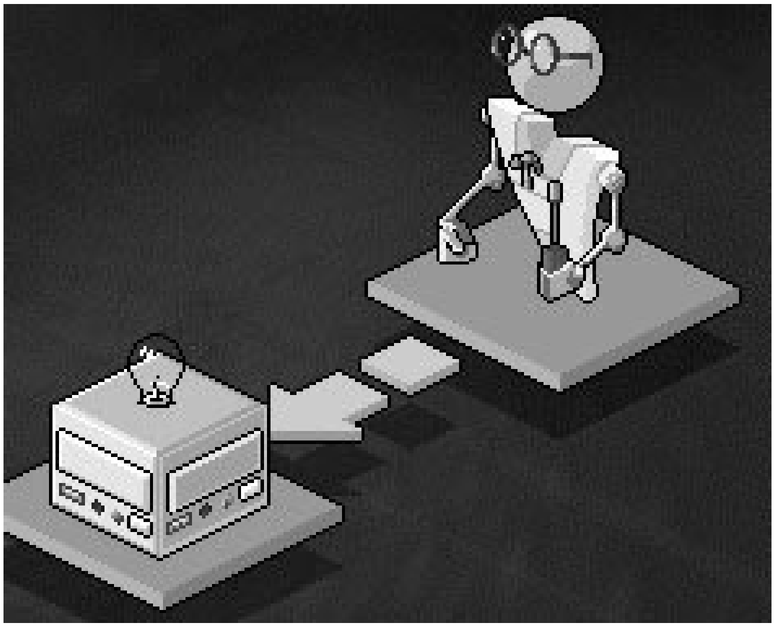

Figure 8–7. *A TDR helps to identify a bad cable using a sonar signal.*

Although a DVM is used primarily to determine if a signal can flow across a cable, it can also be used to search for malfunctions within a network device, such as a router or network interface card. However, it is rarely used in this manner.

The TDR, the oscilloscope, and the DVM are tools used to measure hardware components of the network, but these devices do not give the network support technician any insight into the local components such as data packets.

A **protocol analyzer** and an **advanced cable tester** are used to measure network traffic. This includes counting data packets that are transmitted, counting the number of collisions that occur, counting the number of resent data packets, and measuring the traffic flow across various segments of the network.

Network traffic can radically increase when a network interface card, hub or other network device malfunctions. These devices can saturate the network with broadcast packets called a broadcast storm.

Broadcast storms impede the flow of normal network traffic. When this occurs, network administrators typically receive complaints of poor network performance from users. The protocol analyzer is used to track down the malfunctioning component, which is then replaced.

However, the network administrator can reduce the impact of a broadcast storm by employing routable network protocols and routers on the network. Routers automatically drop broadcast packets.

Therefore, the malfunctioning network device won't be able to broadcast erroneous packets to network segments linked by a router.

■ Summary

The network administrator must develop a good network operating plan to reduce the opportunity for mistakes, mistakes that could disrupt network operations. The plan must consider network security, standardizing procedures, good documentation of those procedures and the network topology, backups of network resources and their locations, and regular maintenance and upgrading of network components.

Network disruptions typically occur when someone that has access permission to the network does something inadvertently to halt network operations. This includes the network support technicians, whose mistakes can be irrecoverable.

The best way to reduce these errors is to establish and strictly enforce access restrictions. Access restrictions limit network resources a person can share and how the person uses those resources.

While network software provides the utilities to limit access to network resources, it is up to the network administrator to implement the access restrictions defined in the network plan.

Granting access to a network resource begins by identifying the owner of the network resource, then letting the owner decide which users can have access to the resource. The owner is probably the best person to weigh the business needs against the need for protection. When someone requests access to a network resource, permission must be obtained from the owner of the network resource before access is granted.

The network administrator should develop a handbook that contains setup and maintenance procedures for every network component. Each procedure should be a step-by-step guide that walks a technician through a process. Most of these procedures can be copied from the manufacturer's documentation.

The handbook should contain the physical location of network components, configurations, floor plans that identify departments, and desk and desk numbers used to identify a user when a trouble call is received.

The handbook should also contain the names and telephone numbers of secondary support staff. These are the people, sometimes manufacturer's reps, who can help the technician resolve problems that are not contained in procedures.

You can't prevent hardware failures, but you can develop a plan to minimize the network downtime when hardware failures occur. And the best approach is to have backups available that can immediately take over for the failed component.

Backups refer to duplicate software and hardware available on site. It is not at all uncommon for an organization to have drop cables, connectors, hard disks, modems, network adapter cards, and even a configured server available to go online at a moment's notice.

A backup plan is costly and may be beyond the economical reality of smaller organizations. The network administrator should conduct a risk analysis to determine how much of a backup plan is needed by the organization. A risk analysis is a review of network operations and components to assess the chances of failure and the economical cost of those failures. Risk analysis must consider these factors:

- How much would the organization lose if a particular component (i.e., a server) became disabled?
- How soon can the malfunctioning component be replaced?
- What is the failure rate of network components?
- Is it economical for the organization to stock replacement components?

Network planning must include scheduled maintenance of hardware. This will extend the mean time between failures of network components. The maintenance schedule of network devices, maintenance procedures, and information when those procedures were performed and who performed them should be kept in a maintenance log.

Network operations must be consistently monitored to give the network administrator an insight into how well the network design meets the needs of the organization. The network administrator should look for clues of forthcoming difficulties so that preemptive action can be taken before users notice a drop in network services.

Network monitors collect and count certain activities on the network and relate them to the time the activity occurred. The information can then be displayed in various ways to help the network administrator analyze network operations.

Once a network is installed and has stabilized, the network administrator should run all the monitors to determine a baseline for the network. A baseline consists of statistics that represent acceptable performance and must be stored for future reference. Network performance is compared to the baseline to determine if the network is operating efficiently. If not, then adjustments can be made to the network to bring network operations closer to the baseline.

Windows NT Server contains a utility called the Performance Monitor that is ideal for tracking network events. The Performance Monitor tracks network performance in real and recorded time.

Each event is called a counter and can be displayed on the screen, saved to a log, or printed in a report. Also, the network administrator can set up a threshold value for each counter. If the value of the counter falls above or below the threshold values, then the Performance Monitor should sound an alarm that alerts the network administrator to the problem.

Another useful monitor you'll find with the Windows NT Server is the Network Monitor, which tracks data packets flowing over the network. The Network Monitor copies data packets into a log. Information in the log can be filtered by network address, data packet type, or by any pattern of characters.

▲ Chapter Review Questions

▲ Fill in the Blanks

1. ______________ ____________ *limit network resources a person can share and how a person uses those resources*

2. *Network downtime caused by a failure of a network device can be minimized by using a ___________ _____________.*

3. *___________ is a review of network operations and components to assess the chances of failure and the economical cost of those failures.*

4. *________ ________ is the number hours of operation before a device is expected to fail.*

5. *________ __________ reduces the likelihood that a network device will break down.*

▲ True/False

1. *(T/F) Network monitors collect and count certain activities on the network and relate them to the time the activity occurred.*

2. *(T/F) From the data captured by the Performance Monitor, the Network Administrator is able to find missing users on the network.*

3. *(T/F) Delivery time of replacement network components should not be considered as part of the network plan.*

4. *(T/F) TDR is a tool used to track down a bad cable by sending a sonar signal across a network cable.*

5. *(T/F) A protocol analyzer and an advanced cable tester are used to measure cable length.*

6. *(T/F) The network administrator can reduce the impact of a broadcast storm by employing routable network protocols and routers on the network.*

7. *(T/F) Combining the current performance level with the baseline performance level will indicate if there is a performance problem.*

8. *(T/F) A performance monitor is used to measure trends in a network.*

9. *(T/F) A cable malfunction to a network card can be identified by using the Time-Domain Reflectometer (TDR)*

▲ Multiple Choice

1. *What is the term used to identify the source of a malfunction on the network?*

A. Frame Analysis

B. Isolating

C. The spy inspector

D. Sonar the network

E. Backing up the system

2. *An event tracked by the performance monitor is called?*

A. Counter

B. Internal check

C. Event modulation

D. Access right

E. Access restriction

3. *What is the term used to describe measurement of the acceptable level of network performance?*

A. Baseline

B. The performance monitor

C. The oscilloscope

D. The specification ratio

E. The 5.3 ISS protocol

4. *What term is used to describe the settings of network devices?*

A. Configuration

B. Sync set

C. RTT adjustments

D. Baseline setting

E. Tweaking the network

5. *What protects the network from users or network staff from making inadvertent mistakes that could cause a network disruption?*

A. Network security plan

B. Background checks of employees

C. Testing potential employees before they are hired

D. System tracking

E. The network controller

6. *The cause of a network problem is called a* ________.

A. bad zone

B. network failure

C. STV error

D. STP error

E. bottleneck

▲ Open Ended

1. How would you use a network monitor to determine if there is a degradation in network performance?
2. What procedures would you use to respond to a complaint from a network user?
3. Describe the ISO's five network management categories?
4. How would you determine if a network malfunction is critical to the organization's operation?
5. How would you go about creating a handbook for network support technicians?