17

TROUBLESHOOTING

When your network is working properly, it's all but invisible; you can send and receive files through the network between any pair of computers or other connected devices. But when a connection fails, or one of your users can't find a network node, or any of a truly amazing number of other possible problems occurs, as the local network expert, it's your job is to fix it. Network problems always have a specific cause (or combination of causes), even if that cause is not obvious.

Too often, a network error message will say something like "ask your network manager for assistance." But when the network manager is *you*, that message doesn't tell you how to solve the problem. This chapter offers some tools and methods that will help you identify and solve most network problems.

General Troubleshooting Techniques

The key to successful troubleshooting is to follow a logical problem-solving process, rather than simply trying things at random until you stumble upon the correct solution to your problem. Most people who spend a lot of their time fixing things use a system like this without a formal plan, but if you're new to repairing computers and networks, consider using the techniques in this chapter as a guide.

Many of these suggestions are common-sense answers, rather than complex technical procedures. Don't overlook them; otherwise you can spend hours tracing a circuit or trying to find a bad connection just because somebody has unplugged a cable.

Remember that a problem that appears in your network might really be located on one of the computers or other devices *connected* to the network. In many cases, you will want to look for problems in the Windows, Macintosh, or Linux/Unix operating system as well as on the network itself.

Define the Problem

The first step in solving a problem should be to identify the symptoms. Remember that computers and networks don't break down completely at random. Every piece of information you can find about a problem can help you isolate and solve it. Is the problem a failure to connect to a particular computer through the network, or an error message, or a file transfer that takes longer than usual? Is it limited to a single computer, or does it appear all over the network? Have any of the lights on your network router, switch, or modem changed color or gone dark? Does the problem occur when you are using a particular program or only when a certain desk lamp (or vacuum cleaner or any other electrical device) is turned on? As you identify symptoms, make a list—either on paper or in your mind.

If you see an error message, copy the exact text onto a piece of paper. You might have to restart the computer or go to another computer to search for information, and you will need the specific wording of the message. Don't ignore the cryptic code numbers or other apparently unintelligible information. Even if the message means nothing to you, it could be the key to finding the help you need.

Sometimes you can identify a pattern in the symptoms. When more than one user reports the same problem, ask yourself what those users have in common: Are they all trying to use the printer or connect to the Internet at the same time? Are they connected to the network by Ethernet cables or Wi-Fi? Does the problem happen at the same time every day?

If you're lucky, defining the problem can tell you enough to fix it. For example, if the Power LED indicator light on your modem is off, that's a good indication that the power cable is unplugged, either at the wall outlet or on the modem itself. If everybody has trouble connecting to the Internet during a rainstorm, maybe water is leaking into the telephone cable that carries your Internet connection from the utility pole to your house (that

happened to me—the repair guy told me that the cable had been there since about 1927).

More often, your list of symptoms will be a starting point that you can use to search for more information. As you analyze the problem, ask yourself these questions:

What caused the problem? Did it occur when you or another user ran a specific program or tried to connect? Does the problem seem to be related to some other action? If you try the same action again, does the same problem occur? Did it first appear when you turned on a computer?

What has changed? Have you installed new hardware on the network or loaded new software on the server or another computer? Did you recently update the router's firmware? Have you made any other change to the network or another connected computer, even if the change seems unrelated to the problem?

What else happened? Have you noticed any other problems or unexpected events? Has another network user experienced a similar problem at about the same time?

Is this a new problem? Have you ever experienced this problem or something similar before?

Look for Simple Solutions First

Look for easy solutions before you start to tear apart hardware or run complex software diagnostic routines. Nothing is more aggravating than spending several hours running detailed troubleshooting procedures, only to discover that restarting a computer or flipping a switch is all that was needed to fix the problem.

Restart Everything

The first thing to try when an otherwise unexplainable problem occurs is to turn off each network component—one at a time—wait a few seconds, and then turn it back on again. Sometimes that's all you need to do to clear a program or a chunk of memory that is stuck on the wrong setting and return it to the correct value. If possible, use the operating system's shut-down process to turn off the computer in an orderly manner; don't use the power switch or reset button unless the computer won't respond to a mouse or keyboard command.

NOTE *Don't turn off your computer until you have copied the text of any error messages on the screen. Sometimes the same problem will produce a different message after you restart (or none at all), and the text of the original message might be a useful troubleshooting tool.*

When you restart a computer, don't use the Restart option; that can leave some settings at the same values rather than resetting them to the default startup configuration. You should turn off the computer completely, count to ten, and then turn it back on.

If the problem continues after you restart the computer, try restarting the modem, Wi-Fi access point, or network router. If a device doesn't have an on/off switch, disconnect the power cable, wait a few seconds, and plug it back in. After you restart each device, check to find out if the problem still exists. If the problem still occurs, move on to the next device.

Check the Plugs and Cables

If a single computer can't connect to the network, confirm that the physical cables providing those connections are not unplugged. Be sure to check both ends of each cable. If the whole network can't find the Internet, check the cables connected to the modem. If possible, examine the cable itself to make sure it hasn't been cut someplace in the middle.

Almost all routers, switches, modems, and network adapters have LED indicators that light when they detect a live connection. If one or more of these LEDs has gone dark, check the connection.

Most data plugs and sockets maintain solid connections, but it's possible that a plug might have come loose without separating itself from the socket, or a wire inside the plug might have a bad contact. If you suspect a loose connection, try wiggling the cable while you watch the LED indicator that corresponds to that socket. If the LED lights and goes dark as you shake the cable, try a different cable.

If you can't connect through a newly installed wall outlet, make sure the wires inside the outlet are connected to the correct terminals at both ends of the cable inside the wall (at the outlet and at the data center).

To quickly confirm that data is passing through the network to and from each computer, use the tools supplied with the computer's operating system to display network activity. In Windows, use the Networking tab in the Task Manager; in Linux, use the `ethtool` command (`ethtool` *`interfacename`* `| grep Link`). If the computer reports that no link is available, a cable is disconnected or the network adapter or hub has a problem.

Check the AC Power

Every device connected to the network probably has an LED indicator that lights when the device is connected to AC power. When a connection fails, look at the front of each device to confirm the power light is on. If it's not, check the device's power switch (if it has one) and both the plug at the back of the device and the plug or power supply that plugs into the AC outlet.

If you use a power strip or an uninterruptible power supply, make sure that the master power switch is turned on and the power unit is plugged into an AC outlet.

If the network fails but your computer still works, a fuse or circuit breaker might have blown in the room containing the network switch, router, or other control device.

Check the Settings and Options

Look for other switches and settings that might interfere with a device's operation. For example, make sure that the network printer is online and that no Error LED indicators or messages are visible in the control panel. Or if you're having trouble with a Wi-Fi connection, make sure your computer hasn't associated itself with the "wrong" base station and connected to one of your neighbors' networks instead of your own.

Isolate the Problem

If your search for simple solutions to a network problem or failure doesn't produce an answer, the next step is to identify the physical location where the problem is occurring. Although it's easy (and often appropriate) to think about a network as an amorphous cloud that exists everywhere at the same time, when you're looking for a specific point of failure, you must replace that cloud with a detailed map that shows every component and connection. If you don't already have a network diagram in your files, consider drawing one now.

Most problems offer some kind of hint about their location: If just one computer's connection to the network has failed, but all the others work properly, the problem is probably in that computer or its network link. But if nobody on the network can connect to any other computer or to the Internet, the problem is probably in a server, router, or other central device. Start searching for the source of a problem in the most logical device.

If you have a hardware problem, it's often effective to isolate the problem by replacing individual components and cables one at a time until the problem goes away. If the problem disappears when you install a replacement, that's a good indication that the original part was the source of the problem. If the replacement is a relatively expensive item like a router or a printer, you might want to send it back to the manufacturer for replacement or repair, especially if it's under warranty. But if you replace a cheap part like a cable or a network interface card, it's often easier to just throw it away and buy a new one.

Similar techniques can work with software. If a computer connection fails, try shutting down each program running on that computer, one at a time, and then try to reestablish the connection. If you recently installed a new program, driver, or update, try uninstalling the new software and test the connection again. If the connection works, the conflict is between the new software and your network connection or device driver. In Windows, try restarting the computer in Safe Mode and re-establishing the connection; if it works in Safe Mode, you know that the Windows operating system is not the source of the problem.

Retrace Your Steps

Even if a network problem appears without warning, the problem was probably caused by something that has changed within the hardware or software. Therefore repeating your steps can often help identify and solve it.

Keep Notes

As you try to identify and solve a problem, keep a record of what you have done. Describe each problem you encounter and what you did to fix it in a simple log or notebook. Note configuration settings, websites that provide useful information, and the exact location of any options or control programs that caused the problem or helped solve it. Keep this on paper, rather than in a text file stored on the computer, so you will be able to access it if the computer breaks down again.

If the same problem appears again, your log will tell you exactly what you did to fix it the first time; rather than stepping through all the same unproductive troubleshooting techniques again, you can go directly to the correct solution.

One excellent approach is to keep a network notebook in a loose-leaf binder. Among other things, your notebook should include the following:

- The configuration settings and passwords for each modem, router, Wi-Fi access point, and other device connected to the network
- The numeric IP addresses for your Internet connection, DNS servers, default gateway, and subnet mask
- The numeric addresses used by your LAN
- The make, model, serial number, and MAC address (if you can find them) of each hub, switch, router, modem, Wi-Fi access point, network adapter, and other network device
- A list of channel numbers, SSIDs, and passwords for your Wi-Fi network
- The telephone numbers and other contact information for your ISP and the telephone company or cable service that supplies your physical Internet connection
- Instruction manuals for each modem, router, access point, or other network device
- A list of your network's users, including names, telephone numbers, and logins
- A diagram that shows how each computer and other device connects to the network
- Passwords for each network server
- Account names and passwords for your email service
- A list of rooms that have wall-mounted network outlets and the label on the other end of each cable
- A log of adds, moves, changes, and deletions to your network
- A log of repairs, including:
  - The date and time each problem appeared
  - A description of each problem
  - What you did to fix the problem

- The time and date of each call to a technical support center
- The name and telephone number of each technical support person you talk to
- The *trouble ticket* number or case number assigned to the problem by each support center

WARNING *Your network notebook might contain confidential information such as passwords and information about user accounts. Therefore, you should to keep it in a secure location such as a locked cabinet or drawer.*

Viruses and Other Nasties

If you can't find an obvious solution to a network problem, it never hurts to run a complete scan for viruses, worms, Trojan horses, and spyware on each computer connected to your LAN. Even if you have firewalls, up-to-date antivirus programs, and other network security software running on all your computers, it's possible that something might have slipped through your defenses.

Several antivirus program vendors offer free online scans that might identify a virus that your resident program might not catch. As part of your troubleshooting routine, run a full scan with your usual network security programs and also use one or more of these online scans:

Trend Micro HouseCall *http://housecall.trendmicro.com*

Symantec Security Check *http://security.symantec.com/sscv6/default.asp*

BitDefender Online Scanner *http://www.bitdefender.com/scan8/ie.html*

Kaspersky Online Scanner *http://www.kaspersky.com/virusscanner*

ESET Online Scanner *http://www.eset.com/onlinescan/*

Panda ActiveScan *http://www.pandasecurity.com/homeusers/solutions/activescan/*

Use an online scanner made by a different supplier from the one that came with the antivirus program resident in your computers. Each company employs a slightly different set of rules for finding and isolating viruses, so you will want to take advantage of more than one approach.

Other Common Problems

It's not practical to describe every possible network problem, but there are a few that occur more frequently than others. If the problem in your network is not described in this chapter, try the Windows Network Problem Solver described in "The Collective Wisdom of the Internet" on page 247 (for computers using Windows), or search for information about the problem in the web pages devoted to your own operating system.

Configuration Settings

When you can't connect your computer to the Internet, but other computers on the same network can connect, check the computer's network configuration settings to confirm that the default gateway and the DNS server are present and correct. If none of the network's computers can find the Internet, check the settings on the network's router or modem.

To confirm that the gateway and the DNS server are alive and operating properly, try sending ping requests to their numeric addresses. If you don't receive a reply, look for a problem in the gateway or the server, or in the equipment and cables between your computer and the target.

DHCP Settings: DNS and Default Gateway

When a DHCP server is active on your network, and your own computer (or the one you're troubleshooting) is set to accept DHCP settings, the computer should automatically connect itself to the network. But if there's no DHCP server, or if the computer is not configured to accept DHCP data from a server and the settings on the computer itself are missing or incorrect, the computer won't connect.

To confirm that the DHCP settings are correct, follow these steps:

1. Check the modem, router, Wi-Fi access point, or other device that normally acts as DHCP server for your network. If the server is active (and other computers on the network are connecting normally), the problem is in your computer; if it's not active, either turn it on or confirm that this network doesn't use DHCP.
2. Open the network configuration settings utility in your computer. If the DHCP server is active, confirm that the computer is set to accept data from the server; if the network does not use DHCP, make sure the addresses for the DNS server and the default gateway (or gateway router) are correct.

If the DNS server settings in your computer or DHCP server appear to be correct, it's possible (but unlikely) that the DNS server itself is not working. Try adding the address of one of the OpenDNS servers (208.67.222.222 or 208.67.220.220) as an alternative to your usual DNS server's address.

Failed Connection to a Specific Site

When you try to connect to a specific website or other Internet service, you will sometimes see an *Unable to connect* message instead of the web page or other screen you were expecting. When this happens, immediately try some other address that takes you to a site in a different geographical location; for example, if you can't connect to *The New York Times* website, try a site based in Germany or Australia. If you can connect to the second address, you can

safely assume that the problem is at the first address, and not in your own computer or network. If you can't connect to any site, look for a local problem such as your computer, the LAN, or your Internet service provider.

An Alternate Connection to the Internet

When your Internet connection breaks down, it's not possible to use that connection to consult technical support websites or send email to your network provider. Therefore, it's often helpful to have a backup method for connecting at least one of your computers to the Internet. It might be a neighbor's Wi-Fi network (with their permission, of course), a nearby library or coffee shop that offers Internet access, or a link through a dial-up telephone line and modem.

Before you have a problem, ask your Internet service provider if they offer dial-up access along with their high-speed services. If they do, ask them for a dial-up account as an emergency backup, and make a note of the access telephone numbers, login name, and password in your network notebook.

The Collective Wisdom of the Internet

Any problem that occurs on your network has happened before to somebody else. You have an excellent chance of finding a description of the problem and instructions for fixing it someplace on the Internet.

This is where defining the problem carefully becomes important. If you're working with a Windows-based network, the Microsoft Knowledge Base at *http://support.microsoft.com/* can be particularly useful; if Microsoft's technical support people have ever had to deal with a particular problem, they have probably included instructions for fixing it in the Knowledge Base. Similar resources exist for Macintosh networks and servers at *http://www.apple.com/support*, and for Unix and Linux systems in the Support sections of each distribution's website.

Other online sources for useful troubleshooting information include manufacturers' technical support centers, independent newsgroups and web forums, and sites such as Wikipedia and HowStuffWorks.com that offer descriptions and explanations of various types of technology. If those sites don't answer your question, try a more general web search. Type a few keywords that describe the problem (such as "XP can't find network printer") or the exact text of an error message into a web search tool and follow each of the links to read about other people's experiences under similar circumstances. Remember that quotation marks around phrases instruct the search sites to search for the entire phrase rather than individual words.

One particularly helpful tool for troubleshooting networks is the Windows Network Problem Solver at *http://winhlp.com/wxnet.htm*, shown in Figure 17-1. The Problem Solver is an interactive list of symptoms that links to instructions for solving the most likely cause of the problem. If you take the time to carefully answer each of the questions in the problem definition form, the Problem Solver can be a remarkably effective tool.

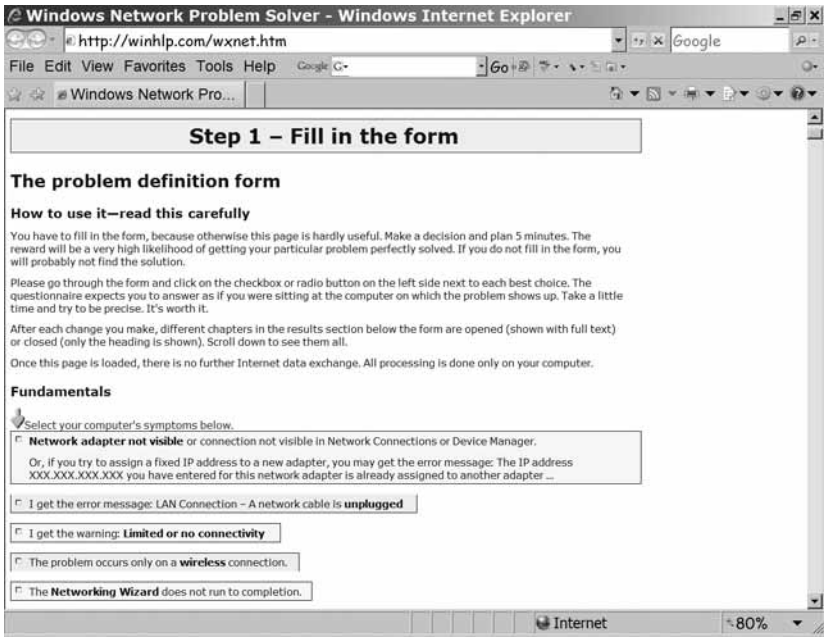

Figure 17-1: The Windows Network Problem Solver is an excellent interactive trouble-shooting tool. This screen image shows only a small portion of the page; scroll down for additional information and instructions.

Software for Troubleshooting

Several software programs can gather and display useful information when you're trying to understand what's happening inside your network. These programs are available as free or trial downloads, so you don't incur a cost when testing them.

Network Magic

Network Magic (*http://www.networkmagic.com/*) provides a graphic display of the devices connected to a LAN, as shown in Figure 17-2, and a central control point for adding new network devices or changing the existing network configuration. It can also perform some basic troubleshooting tests and automatic repairs.

Protocol Analyzers

Microsoft Network Monitor (go to *http://www.microsoft.com/downloads/* and search for *Network Monitor*) and Wireshark (*http://www.wireshark.org/*) are free protocol analyzers that capture and display data as it moves through your network. In other words, they grab each block of data (a *frame*) as it passes in or out of your computer, and they display the contents of the frame along with detailed information about the form and structure of each frame. Figure 17-3 shows a data capture in Network Monitor, and Figure 17-4 shows

a Wireshark screen. The two programs capture the same data stream, but they handle and display it differently. The programs are available at no cost, so you might want to install both of them. Protocol analyzers are also known as *network sniffers*.

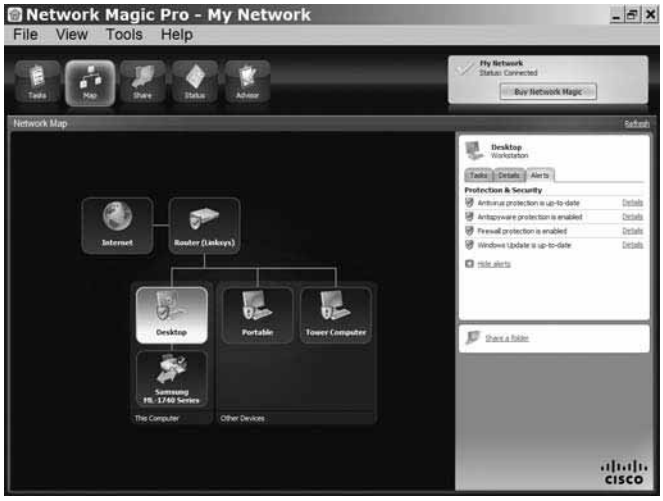

Figure 17-2: Network Magic scans your LAN and displays all the devices connected to it.

Most of this data display looks like hexadecimal gibberish, but it contains the actual text of messages, conversations, and other transactions, along with all the commands and status messages that move through the network. Most of the time, you can allow your computer and the network plumbing to handle the data in background. But when something goes wrong, the data captured by a protocol analyzer can help you identify what's causing the problem.

For example, if the amount of incoming or outgoing traffic moving through your network increases, the network may be sending or receiving many requests every second. This could be a hacker's denial of service attack, or a computer that has innocently latched itself into an endless program loop. Either way, you will want to identify the source and take action to make it stop. When this happened to me, I used Wireshark to find the numeric IP address of the computer that was originating the bogus messages and a whois program to identify that computer's owner; then I sent an email explaining the problem and asking them to fix it. The data stream stopped within an hour.

A network sniffer can also identify a device within your own network that becomes infected or has some other problem that interferes with proper operation. By running the sniffer program on more than one computer, or even inserting a sniffer at a router, a modem connection, or other interface point, you can often isolate the source of a problem.

You won't use a protocol analyzer very often, which is probably okay, because it's a complex and tedious process. But when you need to know what's moving through your network, an analyzer can give you information that you won't find anywhere else.

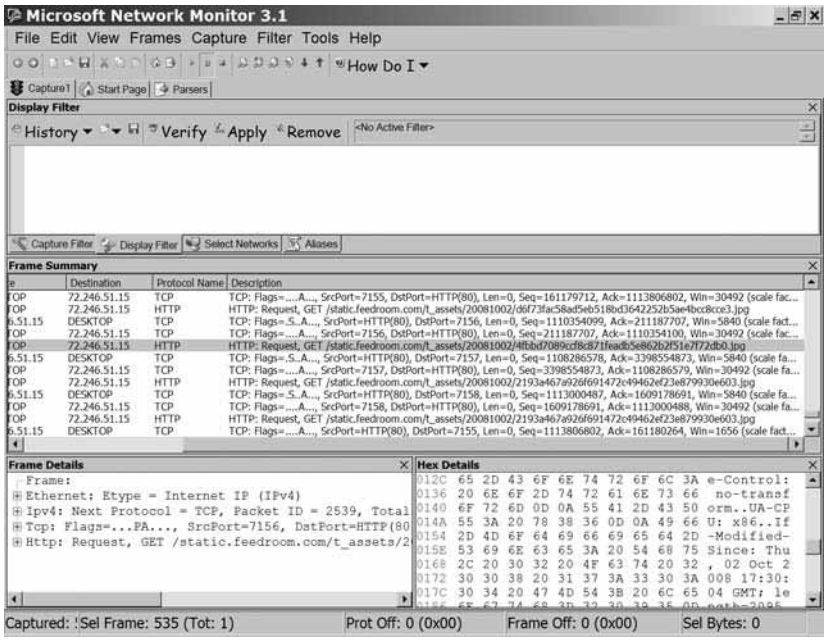

Figure 17-3: Microsoft Network Monitor displays detailed information about network data.

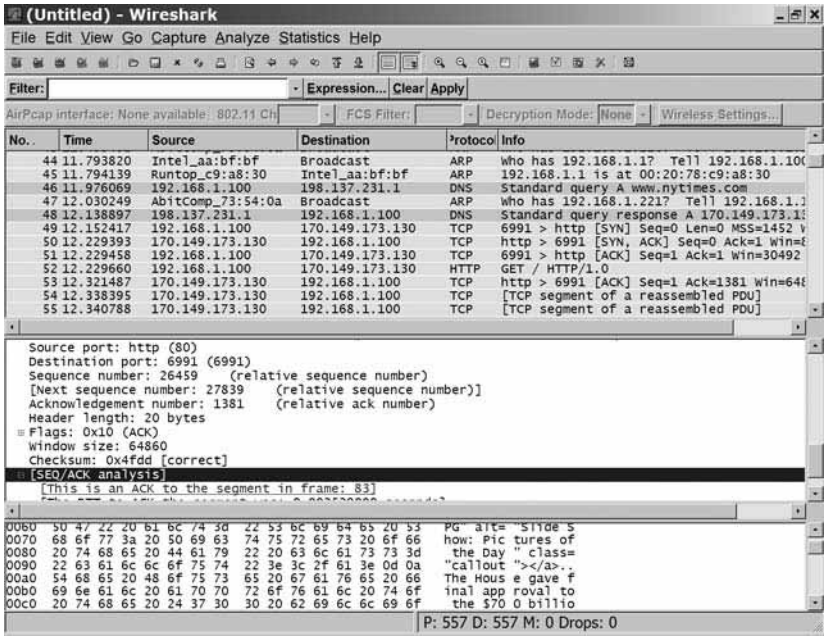

Figure 17-4: Wireshark uses contrasting colors to show different kinds of data frames.

ISP Problems

As a formal or informal network manager, you're often on your own when you're trying to find and fix a problem on your LAN, but if you or one of your users discovers a problem using the Internet, you might need help from your Internet service provider's (ISP's) support center and the people who run the computer or network at the other end of your connection.

Therefore, you should find and keep the telephone numbers and email addresses of the ISP's help desk and the network tech center at the telephone company, cable TV service, or other company that provides the physical connection between your own LAN and your ISP. The people who answer calls in those support centers are there to help you, and they will often have tools that can test and monitor your network connection. When you talk to a support representative, ask for the case number or trouble ticket number that they have assigned to your problem; if you have to call back later, the case number will lead the person who takes your call to the notes about earlier calls.

Don't Panic

Finally, keep calm. Your network does not have a mind of its own. If you take a logical and organized approach to finding the cause of a network problem, you will probably solve the problem without developing (or enlarging) an ulcer. Over time, you will recognize particular symptoms and know how to home in on the most effective diagnostic tools and techniques.

If you can't find the problem after searching for an hour, walk away for a few minutes. Make yourself a sandwich, have a cup of coffee or a glass of lemonade, or go for a short walk. The network will still be there when you get back, and you'll feel better about it. Approaching the problem with a fresh mind can often be the most effective possible way to solve it.