

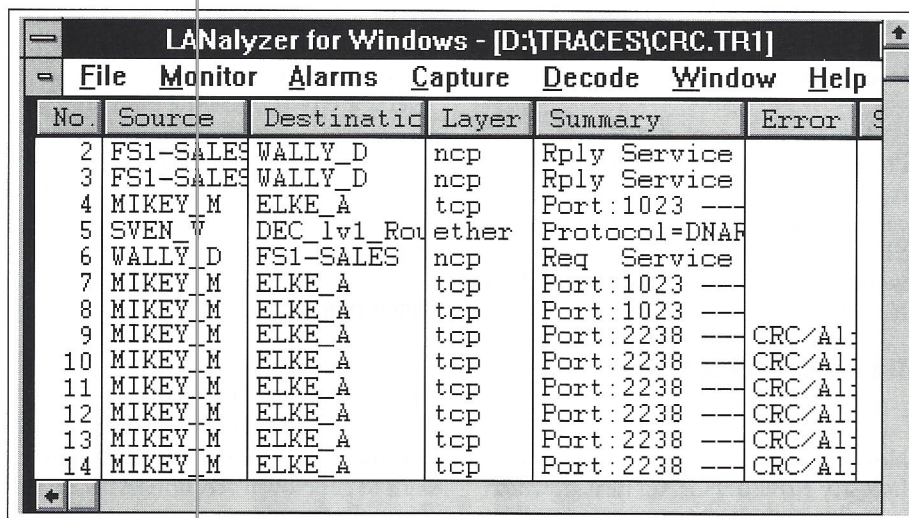
NETWORK BASICS

TROUBLESHOOTING

Identifying and Eliminating Problems on Ethernet Networks

By Laura Chappell

This article is part 1 of a three-part series that focuses on troubleshooting and optimizing Ethernet, Token Ring, and NetWare communications using a protocol analyzer such as Novell's LANalyzer for Windows, NCC's LANalyzer, or Network General's Sniffer. Part 1 highlights Ethernet networks.



No.	Source	Destination	Layer	Summary	Error
2	FS1-SALES	WALLY_D	ncp	Rply Service	
3	FS1-SALES	WALLY_D	ncp	Rply Service	
4	MIKEY_M	ELKE_A	tcp	Port: 1023	
5	SVEN_W	DEC_lv1_Rou	ether	Protocol=DNAF	
6	WALLY_D	FS1-SALES	ncp	Req Service	
7	MIKEY_M	ELKE_A	tcp	Port: 1023	
8	MIKEY_M	ELKE_A	tcp	Port: 1023	
9	MIKEY_M	ELKE_A	tcp	Port: 2238	CRC/A1:
10	MIKEY_M	ELKE_A	tcp	Port: 2238	CRC/A1:
11	MIKEY_M	ELKE_A	tcp	Port: 2238	CRC/A1:
12	MIKEY_M	ELKE_A	tcp	Port: 2238	CRC/A1:
13	MIKEY_M	ELKE_A	tcp	Port: 2238	CRC/A1:
14	MIKEY_M	ELKE_A	tcp	Port: 2238	CRC/A1:

Figure 1: Summary of communications up to the point of the station's disconnection.

Whether your network is large or small, you have probably spent some time trying to resolve communications problems. Using a network analyzer to view network communications speeds up your ability to isolate problems that otherwise could lead to hours of guesswork and frustration. You can also use analyzers to increase performance by optimizing the communications channel or server configuration.

Network analyzers allow you to look directly at the communications occurring

on the network. Many network analyzers offer an automatic error detection system that alerts you to problems or potential problems on the network. For example, if two stations on the network are sending malformed packets because they have a bad driver, a network analyzer sees these malformed packets, increments an error counter, and triggers an alarm.

Various types of analyzers are available. Some analyzers include special hardware and software, while others are

software-based only and can use standard network interface boards. Software-only analyzers, such as Novell's LANalyzer for Windows, are less expensive than the hardware-software solutions. The hardware-software analyzer station (a PC with plenty of processing power and RAM) is placed on a network segment just like a workstation.

Basic analyzers look only at the traffic on the segment they are attached to; they cannot view packets traveling across a network separated by a bridge or router. Some distributed analyzer products, however, allow you to look at communications on a remote network segment. Novell's NetWare Management System (NMS) 2.0 includes the NetWare LANalyzer Agent NLM-based software that resides on a NetWare server. (See review on p. 40.) The LANalyzer Agent software captures packets on segments attached to a remote server and transmits the results to a centralized management console. From one PC on the internetwork, you can do packet capture and analysis on your network in Australia, Japan, New York, and so on. Network General Corporation also makes a distributed version of its popular Sniffer product. A distributed analyzer is a must for larger networks that span multiple sites.

Although network analyzers vary in functionality and complexity, they have some common basic features. Most analyzers graph the amount of traffic occurring on the network over time and report errors relating to malformed frames on the network. These frame errors can be caused by faulty network boards, improperly written network drivers, bad cables, and so on. Some analyzers offer an "Expert" system that defines the troubleshooting steps required to fix problems.

If you are new to network troubleshooting, you should consider a network analyzer that offers a graphical view of your network's health and a practical expert system that lists "how-to" tips for fixing problems. If you are more experienced at troubleshooting, you may want a network analyzer that allows you to capture and buffer network packets. By viewing the communications across the network one packet at a time, you can look beyond the standard communications errors caused by faulty boards, cables, and drivers. By understanding how a protocol, such as NetWare's IPX/SPX, works, you can spot application errors or operating system problems such as an overloaded NetWare server.

The remainder of this article focuses on two Ethernet networks that are experiencing poor performance and intermittent connection problems. It examines the symptoms of the problems (some may seem all too familiar to you) and then explains each step of the troubleshooting process, beginning with isolation and identification of the problem.

Case Study 1: Network Board Gone Bad

Does this sound familiar? The phone rings. "Hello," you answer with a smile in your voice—after all, it is a nice day, and traffic was a breeze this morning. A stressful voice breaks onto the line, "Something's wrong with the network. I'm trying to TELNET to another station, and my workstation's locking up. I've got to get files off the host and print reports. What's wrong?" Sigh. It's going to be one of those days.

The stressful phone call initiated the troubleshooting process. The first step was to determine if the caller, Mikey, could communicate with the network. His workstation could connect to other hosts, but then mysteriously locked up. I asked Mikey

to reboot his workstation and attempt to reconnect to the other host while I tracked his station's communications.


I wanted to find out what was happening on the network when Mikey's station locked up. If his station was communicating, I wanted to see what his station was "saying" before the station locked up. I began capturing all traffic on Mikey's segment. By clicking on the LANalyzer for Windows Packet Capture START button, I began capturing packets on Mikey's segment. Figure 1 shows the summary screen of the communications on Mikey's segment up to the point when he received the error message.

As you can see, packets after number 8 show that Mikey's station suddenly began transmitting bad packets—packets with CRC errors. CRC errors are caused by corrupt packets. Before a station transmits a packet, the chipset on the network board performs an equation on the contents of the packet. The remainder of this equation is sent with the packet in a special field called the Frame Check Sequence (FCS) field.

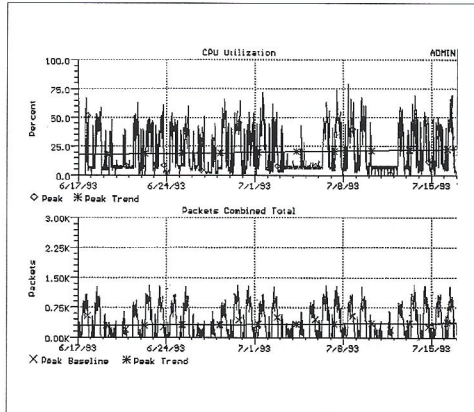
When a station receives a packet, the chipset on the network interface board performs the same equation on the contents of the packet and checks its result against the value in the FCS field of the packet received. If the numbers don't match, the frame is assumed to be corrupt. The receiving station discards the packet.

When a large number of CRC errors are attributed to a single station on the network, it indicates that the station's network board is bad. A simple way to check this is to replace the sending station's network interface board and track the communications again. I replaced Mikey's network board, and no CRC errors occurred on the network and Mikey could communicate on the network again. This problem was simple to fix because we could see the packets Mikey was sending on the network.

If you cannot identify a network error, however, LANalyzer for Windows includes NetWare Expert. NetWare Expert describes the problem, lists possible causes, and suggests troubleshooting methods.



Graphical Workload Analysis with



PINPOINT PROBLEMS

Now you can easily determine growth trends of major file server components and effortlessly pinpoint potential problems before they occur. TrendTrak's highly optimized NLM/VAP provides unattended capturing of file server statistics for integrated graphing capabilities at your workstation.

GRAPH TRENDS

Integrated graphing capabilities include baselines, trends and much more, making workload analysis a snap. You would be hard pressed to find the capabilities offered by TrendTrak at ten times the price!

OVER 40 STATISTICS AND RATIOS

To get your line utilization for the hours of 8AM to 5PM during last month is as easy as 1-2-3: **1**-select the statistic; **2**-set the duration and hours for analysis; **3**-select display or print. It's that simple! No more hardware setup and spreadsheet hassles. Line utilization is just one of over 40 unique statistics and powerful ratios - right at your fingertips!

For NetWare v2.15, v2.2, v3.11, v4.0

For more information call: 1-800-233-7494
619-695-1900 FAX: 619-271-4989

Intrak, Inc. 9999 Business Park Ave. San Diego, CA 92131

Circle 12 on reader service card.

Case Study 2: The Overgrown Network

Users become accustomed to a certain rhythm on the network. They type "WP" to launch WordPerfect and expect the application to come up within a certain amount of time. When there is a delay before the application launches, users notice. Recently, I worked on a large Ethernet network that showed signs of being overloaded. Users complained about performance regardless of the server they worked on. They had also received error messages indicating errors sending and receiving on the network.

The LANalyzer for Windows dashboard indicated that the network was overloaded. The utilization exceeded the alarm threshold (59 percent), and fragments were common (9 percent errors).

Other symptoms also indicated an overloaded network. First, we looked at the typical network utilization over time (trend graphs) and noted whether the network was experiencing a gradual increase in network utilization or a sudden, sharp increase in utilization. This network generally only experienced 12 to 14 percent utilization.

On most networks, utilization gradually increases as users begin using more network resources, such as electronic mail, network printing, and file sharing. A sharp increase in utilization indicates an out-of-the-ordinary condition and should be checked. For example, when new Macintosh users are connected to the network, they may back up their local drives to the server, causing a sudden increase in network utilization. Performing this task at off-peak times will reduce the impact on network performance.

If clients begin to timeout when accessing the network, they will receive error messages such as "Error Receiving on network xxxx" or "Error Sending on network xxxx." These messages indicate the user did not receive a reply to a data request or could not even get a request onto the busy network cabling system.

Trying to communicate on a network that is experiencing high utilization is similar to driving down a Los Angeles freeway at 5 p.m. on a workday—traffic is so heavy it takes longer to get home, and accidents are common. In the same way, when two or more stations transmit on the

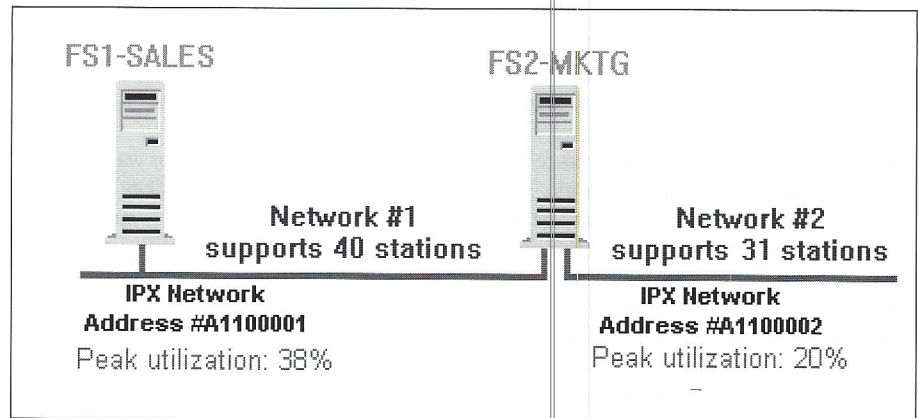


Figure 2: Load balancing two network segments.

cable at the same time, the packets collide. The result of these collisions in Ethernet is fragments on the cable.

If the cabling system cannot handle the load, you can split the network using a router. On NetWare networks, you have two choices: install a new router device on the network or put another board in the server to turn it into a router. In the interest of time and money, I opted for the latter option.

Before I split the network, however, I needed to know which stations communicated with which server. This information helped me load balance the network to reduce excess traffic on one segment.

I set up LANalyzer for Windows to capture traffic to and from FS1-SALES and to send this information to the Station Monitor screen. Then I identified stations communicating with FS1-SALES and the frequency of the communications. I set the Station Monitor screen to sort by the Kbytes/out column. I selected File > Print to record the results.

I performed the same test using FS2-MKTG in the capture filter. By viewing the Station Monitor screen, I identified stations that were communicating most often with FS2-MKTG and printed the results. After studying the printouts, I noted the following:

- 21 stations communicated with only FS1-SALES.
- 19 stations communicated with both FS1-SALES and FS2-MKTG.
- 31 stations communicated with only FS2-MKTG.

Based on this information, I sketched a new network layout, making sure traffic was balanced between two network segments. I installed a second Ethernet board in the FS2-MKTG server and placed the 31 stations that communicate only with that server on the new segment labeled Network 2. The clients that used FS1-SALES and the clients that used both servers were placed on Network 1.

Figure 2 shows the new utilization percentages for each network. The new networks are significantly less busy (38 percent and 20 percent utilization), and the difference in performance is noticeable. Users type "WP" and the program launches within the time frame expected.

When you split a network to improve performance, evaluate how the servers and resources will be used. You should split the network based on the amount of traffic each user creates on the network. A network analyzer is the most accurate method for determining user traffic levels.

This article showed how to resolve two common troubleshooting situations on an Ethernet network using a network analyzer. The next article in this series will focus on troubleshooting a Token Ring network.

Laura Chappell is president of ImagiTech, Inc., and is a principal of the Technology Consortium in San Jose, California. Laura researches, writes, and lectures on network troubleshooting and optimization. ■