

# Network Edge

Competitive Advantages From Data Communications

## Executive Summary

# Focus On The Physical Layer

*A proactive approach using continuous monitoring can prevent downtime.*

It's not an overstatement, anymore, to say that the network has become the business, and the business has become the network. Workstations, personal computers, servers, and other nodes on a local area network (LAN) have become part of the mission-critical central nervous system of most organizations. The high-profile role of networks in large organizations today demands a high level of reliability, similar to that achieved by the local telephone company or electric utility.

Indeed, when LANs fail, the cost is large and growing: Infonetics Research estimates that the annual revenue loss of the average large company due to LAN downtime will increase from \$3.85 million in 1993 to \$22.8 million in 1997 (See Fig. 1).

Among the most troublesome—and expensive—causes of network downtime are problems at the physical layer. Constant moves, adds and changes invariably lead to cable and connector faults. Furthermore, companies making the transition from 10Mbps to 100Mbps Ethernet have discovered that the higher-speed transmissions are more susceptible to cable- and connector-related anomalies. In addition, a growing number of emissions sources can corrupt network traffic. Traditional LAN monitoring tools cannot completely identify or isolate such problems, so it can take hours or days to identify and resolve them.

However, IS managers and senior executives anxious to avoid further losses from network outages, and unable to view these problems with protocol analyzers and remote monitoring probes, have a new option. The NEWSLine product family provides a new level of local area network protection.

### Network Reliability Gets Physical

Physical layer defects that went unnoticed in a 10Mbps Ethernet environment can capsize a 100 or 1,000Mbps network ..... Page 2

### Cabling Woes

Is Category 5 cable incapable of 100 Mbps? .....Page 3

### NIC Knocks

Deviate chips may foul a 10/100 Mbps Ethernet environment .....Page 4

### EMI/RFI Pollution

EMI/RFI problems can plague higher-speed Ethernet implementations .....Page 5

### More Challenges

More users are demanding that network managers guarantee specific levels of service .....Page 6

### Limits of Traditional Monitors

RMON probes and protocol analyzers have blind spots .....Page 7

### An Effective Alternative

NEWSLine uses digital signal processing to continuously monitor all events on a network .....Page 9

### Beta User Report

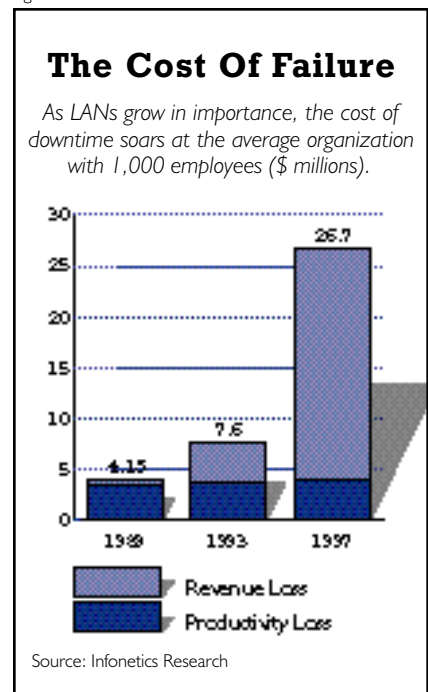
"I can see the true root cause of network problems for the first time." .....Page 11

### About This Report

.....Page 12

Network Edge is a publication of the Network Products Division of LeCroy Corp., Burlington, Mass. Entire contents copyright 1997. © All Rights Reserved. For more information about the report, please see the back cover.

Fig. 1



# Network Reliability Gets Physical

Physical layer defects that went unnoticed in a 10Mbps Ethernet environment can capsize a 100 or 1,000Mbps network.

By Lee Sustar and Larry Marion

The rise of the client/server architecture, and the universal adoption of the Internet and network-centric computing, have radically changed the mission of network managers. Currently 84 percent of corporate personal computers are connected to a LAN, up from 18 percent in 1992, according to a survey by Sentry Research and Analyst Services of Westborough, Mass. The average large company is expected to have more than 2,800 PCs, printers, servers, switches, routers, and other devices on its LANs in 1998, up 40 percent from the census this year, according to a survey by Infonetics Research, Inc. of San Jose, Calif.

Not only are there more users of local area networks, but the role of the network has changed. It is not longer a plaything of the IS department, but the vital pipeline for an organization to conduct business. LANs enable businesses to operate more efficiently by reducing the number of administrative layers and by establishing direct linkages between suppliers and customers. A survey last year by the International Data Corp. market research firm found that 72 percent of managers said their networks were mission critical. "Networks have become more critical to business," notes Rick Villars, an IDC analyst in Framingham, Mass.

As the corporate LAN has become the primary conduit for mission-critical corporate applications, its physical reliability has become a key network management issue, Villars says. The average number of workers affected by network outages has soared during the past several years. Last year the average network interruption due to physical layer failure impacted 116 users, according to IDC, up from 59 employees in 1994 (See Fig. 2). In addition, they're off-line for a longer period of time due in part to the increased complexity of troubleshooting larger networks: IDC reports that the average number of hours of lost

user productivity due to physical layer failure was 101 hours last year, triple the figure for 1994 (See Fig. 3).

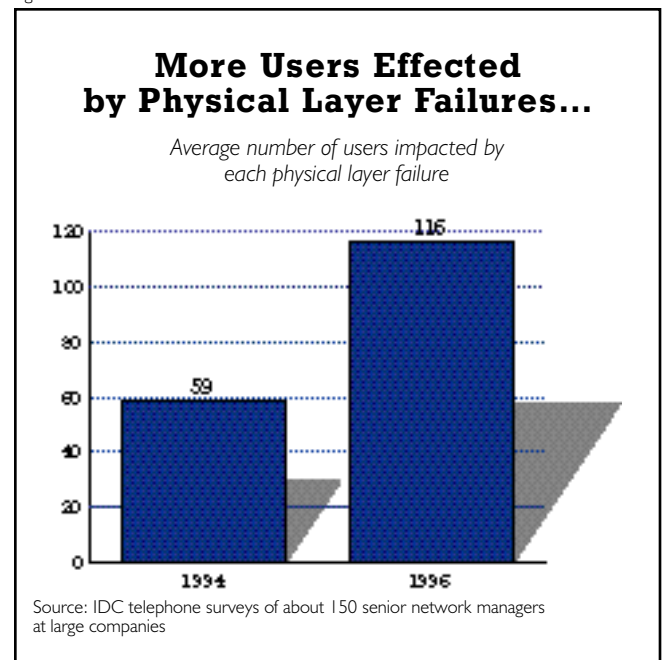
## Network Clog

What's worse is the growing number of physical failures that affect vital business operations. The IDC survey found that from 1994 to 1996 the average number of disruptions of vital networks due to physical network faults increased by more than 37 percent, to 4.7 events in 1996 from 3.42 in 1994.

"If you have a problem that sits on a computer, the first

**Each failure at the physical layer impacted on average 116 users in 1996.**

Fig. 2



place you'll see it is when it shows up across the network and affects a lot of people," noted Michael Howard, Infonetics' president, in a recent issue of *InfoWorld*. "When something clogs the network, it's important."

For example, network outages have a significant financial impact. "People often quantify the outages in terms of lost human resources—the person-hours it takes to retype something," explains Frank Dzubek, principal at Communications Network Architects, a Washington, DC consulting group. "But the real impact is at the corporate level. If an outage affects a workstation running a banking application that's trading currency, you can be talking about literally billions of dollars in losses."

Indeed, one financial services firm has quantified the cost of network downtime, and it is staggering. Officials of credit card processor National Processing Co. of Louisville, KY calculate that each minute of LAN downtime could cost the company \$6,000 in delayed payments and penalty fees. Over the course of a year, the cost of downtime for the company could reach \$170 million, according to a recent issue of *Information Week*.

For the average large corporation, the financial risks may not be as large as those experienced by a bank or securities trading firm, but they are significant and growing. A company with more than 1,000 employees on LANs can expect to lose an average of almost \$27 million a year due to network downtime, according to an Infonetics Research study. Most of the loss—almost \$23 million—is due to revenue losses (See Fig. 1, on page 1).

IDC has quantified the impact of a network physical layer fault in a way that managers will find useful when preparing a proposal to improve their network monitoring and troubleshooting capabilities. Based on surveys of network managers, IDC estimates that the average cost of each physical layer failure is about \$250,000 per 100 users.

The mounting costs of physical failure in networks have focused network managers' attention on the three leading causes of such outages: faulty cabling and or connectors; failures in hubs, network interface cards (NICs) and other active devices; and disruptive levels of electromagnetic or radio frequency interference (EMI/RFI) (See Fig. 4, next page). Each of these three problems are exacerbated by higher LAN speeds. Furthermore, in combination they can be devastating.

## Cabling Woes

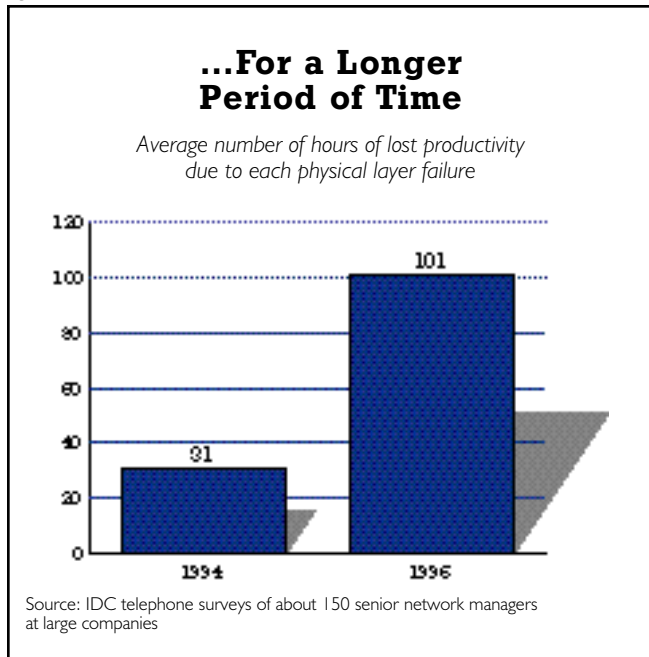
When network managers sweat cable problems, most of the time they're working on Category 5, unshielded twisted pair (UTP) cable, available in more than a 100 different designs from numerous manufacturers. Category 5 UTP is the most common grade of copper cable in use today, with more than 7 billion miles installed in North America, according to analysts, roughly 40 percent of all cable.

**The cost of each physical layer failure is about \$250,000 per 100 users**

Four different types of problems affect the performance of Category 5 cable. The most common are installation mistakes, followed by improper moves, adds and changes; substandard cable materials; and substandard connectors. While some of these problems may have been discovered and corrected after the initial installation for 10 Mbps service, most lie dormant until a network upgrade to Fast Ethernet (100 Mbps), asynchronous transfer mode (up to 155 Mbps) or Gigabit Ethernet (1000 Mbps) is attempted. Frank Coletto, vice president of marketing at Anixter, Inc., a distributor of communications systems and components, warned in a recent edition of *Network World* that a third to a half of Category 5 installations may not be capable of delivering 100 Mbps even though they were able to transmit at 10 Mbps.

**Installation errors.** Many installation mistakes were due to a lack of standards. Dave Stoner, manager of market development at LAN equipment maker Allied Telesyn, Inc. of Bothel, Wash., noted in a recent issue of *Network World* that early Category 5 installations were not necessarily properly implemented, due to the fact that the installation standards were issued after many implementations were made. "Anecdotally, the word is that when it comes time to upgrade to 100Mbps Ethernet, Category 5 cable

Fig. 3



*A third to a half of Category 5 installations may not be capable of delivering 100 Mbps*

doesn't work!" says IDC's Villars. "This has nothing to do with the quality of the cable, but how it was laid."

Although Category 5 UTP cable has been available for almost a decade, standards describing performance and installation requirements were not drafted until 1991 and not really formalized until 1995, noted Anixter Inc. officials Jim Serenbetz and Pete Lockhart in their white paper, "Category 5: How Did We Get Here and Where Do We Go Next?". As a result, a lot of improperly installed cable is buried in walls and ceilings of offices and factories around the world.

**Four out of 10 connectors sold as Category 5 fail to meet specifications**

Poor installations didn't end when the standards were promulgated, though. Many installers failed to follow the standards and specifications even after they were available and clear. "The work undertaken by installers falls way short of the mark," noted author Stephen Saunders in *The McGraw Hill High Speed LANs Handbook*.

A variety of bad installation habits contribute to Category 5 cable inadequacies (See Fig. 5, next page). "Any one of these slip-ups can spell trouble for high speed transmissions," contended Saunders.

**Moves, adds and changes.** Moves, adds and changes have been a pain for network managers for more than a decade, and the increased velocity of shifts in organizations these days, along with the migration to higher speed networks increases the discomfort. According to surveys done for connector maker

AMP, Inc. of Harrisburg, Pa., these shifts can affect 50 percent of an organization's staff each year. For a large organization, that translates into thousands of cabling changes a year, each one capable of creating a physical level failure. And while the incorrect radius of a patch cable may not have an impact at 10 Mbps, it will almost certainly cause problems at 100 Mbps.

**Substandard materials.** Another ticking time bomb is substandard cable. Inconsistencies in the quality and performance of Category 5 cable didn't end when industry standards were adopted. Surging demand for Category 5 UTP led to shortages of critical materials beginning in 1994, especially a form of Teflon known as FEP. Some manufacturers produced Category 5 cables using less FEP on one of the twisted pairs and mixed with other materials that were compliant with the standard but yet exhibited varying electrical performance characteristics, noted Serenbetz and Lockhart in their white paper. Since higher-speed LANs use both twisted pairs, certain cables that were made with less FEP are likely to cause trouble.

**Substandard components.** Upgrading a network to higher speeds also uncovers performance issues related to either the connectors and the wall-plate terminations. Often these components do not meet the same performance standards as top-grade Category 5 cable, and higher LAN speeds inevitably increase the risk of physical faults, noted Frank Bisbee in a recent issue of *Cabling Business* magazine. As signal frequencies exceed 100 megaHertz (MHz), the network generates more bit errors, which "often lead to garbled

Fig. 4

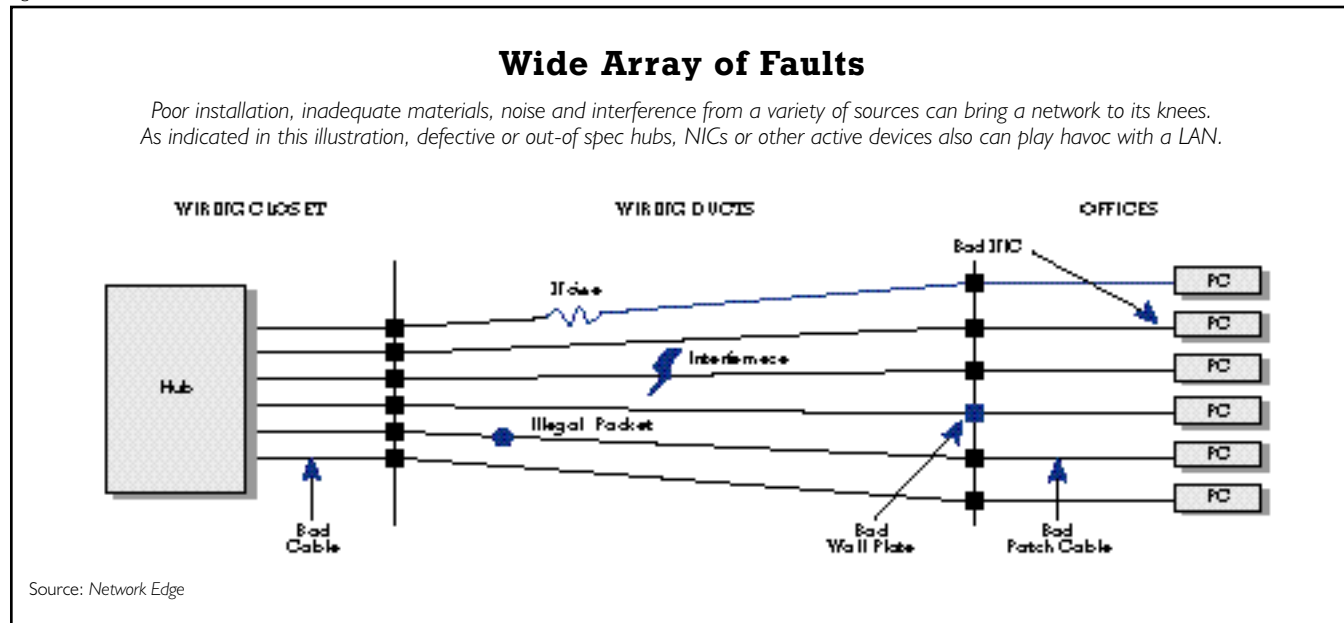


Fig. 5

### Installation Traps

*Inadequate or incomplete specifications, lax installers and other pitfalls can diminish the ability of Category 5 cable to carry higher speed signals. Here are four installation gotchas:*

- 1. Excessive untwisting of the pairs prior to insertion into punchdown blocks. The maximum allowed is 13 millimeters;**
- 2. Failure to adhere to the maximum bend radiuses (less than four times the diameter of the cable);**
- 3. Overcinching of cable bundles; and,**
- 4. Grounding problems**

Sources: Network Edge, The McGraw-Hill High-Speed LANs Handbook

information and or retransmissions of the data," he stated. Saunders noted that independent lab tests found that four out of 10 connectors sold as Category 5 compliant failed to meet specifications. Several others were borderline.

## NIC Knocks

Another complex physical layer challenge is finding faulty NICs and other active devices. NIC failures are relatively rare today. Yet a NIC needn't fail to degrade network performance. Vendors interpreted Ethernet specifications differently, and devices at variance from the standard have had an impact on operations at 10 Mbps and can have severe consequences in Fast Ethernet deployments.

Many problems are rooted in manufacturers' apparently minor deviations from standard specifications, says Diane Myers, senior analyst at In-Stat, a Scottsdale, Ariz., market research and consulting firm. "You get a lot of problems in the chips because it is very hard to integrate mixed-signal, 10/100 products at the physical level," she explains. "Some manufacturers deviate from the standard to integrate the functions of 10 and 100 Mbps, especially if they don't have the design expertise" to do it correctly, she says.

The most common difficulty is failure to meet the standard .96 microsecond interval between packets at 100 Mbps, Myers adds. "The problem is in the clock recovery device within the chips themselves," complicated by the 10/100 integration process, she says. If the interval is off, performance suffers, according to Optimized Engineering Corp., a Palo Alto, Calif.

consultancy specializing in network issues. "Without the interframe gap, it is possible that a station would miss a frame that was destined for it because it had not yet cycled back into receive mode...The problem arises when cards with smaller interframe spacing are mixed on a network with cards that meet the specifications. In this case, there is a potential for lost data. The moral of this story is that a network administrator needs to know what is going on in his or her network and be aware that not all vendors will stick to the specs."

This situation will bring back some painful memories for some network managers. They will remember that the interframe gap problem happened during the introduction of the 10 Base T environment, as it took a few years for some chip makers to master the intricacies of the standards. (For more information about what Ethernet inventor Robert Metcalfe called the "chip-bug scandal," see the March 14, 1994 edition of *Infoworld*, page 46. A research paper on the subject is available from Xerox Parc researcher Wesley Irish at <ftp://ftp.parc.xerox.com/pub/wirish/ethernetnews.posted>.) Whenever a new networking protocol is introduced, these problems are likely to re-occur. In fact, experts say the ramp-up of 100 Base T is triggering similar interframe gap problems.

Even cards that function perfectly well at 10 Mbps can cause massive problems at 100 Mbps due to variations in implementation of the Ethernet standards. Although the IEEE 802.3 standard specifies an "autonegotiation" protocol so that stations can determine which standard to use, not all manufacturers have implemented it, which means the protocol can become a source of disruptive jabber. Specialists at Optimized Engineering explain: "If Ethernet incompatibility jabber were to occur between 100Base-TX and another flavor of Ethernet, the results could be catastrophic" as the idle signal could busy out a 10Base-T or 100Base-T4 network segment. Given that most Fast Ethernet implementations will coexist with 10 Mbps networks, this represents a significant threat to network health.

One new NIC problem that arises at 100 Mbps over Category 5 UTP is due to a change of encoding. Instead of the Manchester encoding used in 10 Mbps, a more efficient scheme called Multiple Level Transition-3 (MLT-3) is used. It is a pseudo 3-state alternating wave as the base waveform rather than the two-state wave used in 10 Mbps Ethernet. Because it is not DC-free, MLT-3 is susceptible to base line wander, which can cause packets to drift out of range of the receiver, resulting in lost data.

Higher speed transmissions challenge NICs in a variety of ways. The faster rise times of NICs operating at 100 Mbps — 2.5 nanoseconds compared to 25 in 10 Mbps networks —

**Higher speed transmissions challenge NICs in a variety of ways**

*“We lost an entire day of production because of one failed NIC”*

reduces the window for successful transmissions. The higher speed also puts more pressure on transmitters to handle data at 40 MHz, increasing the likelihood of lost data.

As signal frequencies exceed 100 megahertz, the chips inside NICs can cause other problems. The equalizers in the components (designed to amplify signals in a network to overcome attenuation of the higher frequencies) also amplify the noise. As a result, higher speed networks can generate more “bit errors,” which “often lead to garbled information and or retransmissions of the data,” noted Bisbee.

NIC performance issues at 100 Mbps are likely to get more attention soon. Justin Smith, a senior analyst at IDC Corp. in Framingham, Mass., argues that only between 10 and 20 percent of 10/100 NICs are running at the higher speed today. However, a surge in the number of users of 100 Mbps is expected soon. “A year from now, everything will be enabled with Fast Ethernet,”

says Mark Christiansen, an Intel Corp. vice president in charge of NICs and other communications products.

In this context, NIC performance problems are expected to increase in the number of instances as well as the number of users affected. Warns Communications Network Architect’s Dzubek, “it

is good if you have the ability to isolate and identify a NIC.”

Indeed. “In one recent job for a large record company, we lost an entire day of production because of one failed NIC,” recalls. Allyson Smith, a Los Angeles-based consultant with First Technical Aid Corp., a national firm specializing in on-site networking and systems support. “This was in a network of 8,000 users, many of whom were trying to make deadlines for ad placement and for other projects.”

Replacing the NIC was easy. Locating it was not. “The problem was that we had few options but trial and error,” she says. “We simply didn’t have any monitoring or testing equipment that could do the job quickly and efficiently.”

## **EMI/RFI Pollution**

Detection and solution of EMI/RFI problems also requires sophisticated equipment. While Cat 5 UTP cable offers limited immunity to external noise such as electromagnetic interference and radio frequency interference, EMI/RFI can be disruptive under certain conditions, such as when external power sources are near the cable. EMI sources are plentiful and usually hidden in most office environments (See Fig. 6).

While eliminating the problems aren’t difficult, pinning them down can be tough. “Noise, however, can elude even the most

Fig. 6

### **Many Sources of EMI/RFI**

*While many sources of interference are obvious when troubleshooting a network, some are not so obvious. Here’s a sampler:*

<b>Obvious</b>	<b>Not so obvious</b>
Elevator motors	Copiers
HVAC motors	Laser printers
Dimmer switches	Cellular telephone base stations
Computers	Wireless LANs
Fluorescent lighting	Televisions
X-ray machines	Microwave ovens

Source: Network Edge

skilled technician, especially if it is intermittent,” noted Chuck Siebuhr in a recent issue of *Cabling Business* magazine: “Testing for noise in some cases may require studies using sophisticated and expensive transmission test equipment”—equipment that networking staff typically do not have on premises. Network managers often track EMI/RFI using trial-and-error methods, beginning with the selection of a test link that recreates normal business conditions. Since such tests are inevitably disruptive and time-consuming, merely attempting to locate the problem can actually magnify its impact.

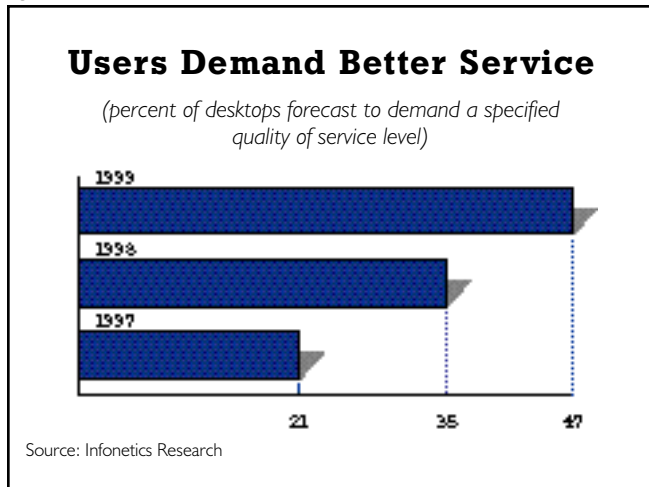
Another EMI/RFI detection challenge occurs in wiring closets. Stacked hubs are typically linked via twisted-pair drop cable. This provides an efficient and inexpensive connection, but also tends to increase the level of interference, notes Dzubek. Such disruptions can take down the entire stack of hubs. Determining which cable is the culprit can be a frustrating and time consuming task, given the rat’s nest of cables in most wiring closets.

Stepping up to 100 Mbps or Gigabit LANs only compounds the EMI/RFI problems in wiring closets and even in standard plenum runs.

What’s behind this problem? David Greenfield of *Data Communications* magazine explained in a recent article that “In general, conductors become much better antennas as frequencies increase, which is why EMI becomes more of a problem in LANs operating at higher speeds.” In fact, Saunders noted, data susceptibility to EMI increases in proportion to bit rate.

Since Category 5 UTP cable is the most cost effective alternative in wiring office buildings, it is becoming more imperative for network managers to adopt testing and monitoring technology that can detect EMI/RFI effectively in UTP as their organizations

Fig. 7



upgrade the speed of their infrastructure. Such a course requires that testing equipment keeps pace with changes in LAN technology, Siebuhr wrote. "As high-speed, high-performance networks become more technologically advanced, so must test equipment and troubleshooting knowledge...It simply makes sense to invest a little extra investigative time up front rather than spend countless hours of downtime and troubleshooting."

Improved test equipment and additional knowledge also are required to manage emissions from higher speed LANs. As noted earlier, UTP system designers turned to MLT-3 line coding to enable Category 5 cable to carry 100 Mbps. However, MLT-3 line code spectra extends well beyond the 100 MHz specifications of Category 5 cable, noted engineers at Optimized Engineering Corp. The consequence is that jitter and inter-symbol interference increase as the upper end of the spectra are attenuated or filtered out by the cabling system. Therefore, high speed data transmission on UTP is a delicate balance between radiated emissions requirements and bit error rate performance, they added.

## Performance Headache

All of these physical layer issues leave networks vulnerable to another problem, dropped packets. And dropped packets severely diminish network performance. "A single lost packet will cause an application to stop dead in its tracks," warned consultant and columnist Kevin Tolly in a recent edition of *Network World*. Robert Metcalfe, the inventor of Ethernet, estimated that a 1 percent drop in Ethernet packets correlates to an 80 percent drop in bandwidth.

Metcalfe, and other groundbreaking LAN developers, coined the term "drop-rate magnification" in 1994 to describe

how the performance of fragile network software might degrade quickly when dealing with a few packets dropped without hardware notice. If one in 10 packets sent per acknowledgment was silently dropped, all 10 might need to be re-transmitted. And each of those transmissions might take 100 to 1,000 times longer than re-transmitting packets whose loss is reported in hardware.

In the three years since Metcalfe and the "elders" made their observation, countless networks have been exposed to the drop-rate magnification problem as the number and compatibility of applications has increased. In part, the problem is due to the fact that dropped packets are enormously difficult to detect because traditional tools often fail to detect dropped Ethernet packets. The precision of remote monitoring (RMON) probes relies on their being able to capture every packet that travels the segment. Precision is decreased when packets are dropped.

## More Challenges

Given the increasingly strategic role of LANs in enterprise applications, more users expect to encounter such problems in the near future as they shift to higher speeds: 76 percent of network users expect 100BaseT to have the same or more failures as with 10BaseT; for switched technology, the respective figure is 63 percent, according to a survey by IDC. To protect themselves and their organizations from the impact of the future failures, more and more users are demanding that network managers guarantee specific levels of service. While only 21 percent of desktops were covered by quality of service agreements this year, network managers polled by Infonetics Research last year predicted that 47 percent of desktops would be covered by 1999 (See Fig. 7).

Ellen Carney, principle analyst of network integration and support services at the Dataquest Inc. market research firm in San Jose, Calif., says that users are correct to assume that the spread of advanced applications will put additional physical strain on networks. "Capacity is the main thing," she says. "How much Internet traffic will there be? Will there be electronic commerce applications?" LAN monitoring must proactively safeguard network capacity to maintain the throughput needed for these and other applications, says Carney, because "people have a tendency to underestimate their needs."

Yet users demand ever-increasing throughput and consistent high performance. Indeed, managers insist on virtually 100 percent uptime. Hence a major contradiction between expectation and reality, since relatively few networks actually achieve 100 percent uptime.

**Network managers put increased emphasis on proactive management.**

## RMON probes can't identify the physical source of network problems

To better fulfill the quality-of-service expectations of users and senior executives, network managers are putting an increased emphasis on proactive management. This approach requires an in-circuit, physical layer view of the network to measure performance and predict outages in addition to isolating and correcting problems immediately. The difficulty for network administrators, though, is that traditional network monitoring solutions were not designed to provide such a solution.

### Limits of Traditional Monitors

LAN monitoring technologies such as cable testers, remote monitoring (RMON) probes and protocol analyzers are used to provide network managers with an instant picture of network performance. RMON probes are embedded in network devices, while portable protocol analyzers and handheld cable testers are directly connected to the network and to individual devices on it.

**Cable testers.** Hand-held cable testers are popular for field technicians and installers. They measure the functionality of Category 5 cables and "deliver easy to understand test results," noted Saunders in *The McGraw Hill High Speed LANs Handbook*. And they are inexpensive, relative to the cost of other approaches.

However, cable testers aren't considered reliable. They "have a wider margin of error," noted Saunders. "In some cases, this has led to network managers and installers failing cable links which were actually Category 5 compliant." Moreover, the testers can't go beyond the wall plate to verify an entire channel. Nor can the devices measure the true impedance of a cable or even take measurements above 150 MHz.

**RMON probes.** RMON-compliant probes are designed to collect and store data for a single segment and to summarize the data according to the types of packets. RMON probes offer statistics on the amount of network traffic such as CRCs and collisions. This helps identify the most frequent network users, tracks bandwidth utilization, and records device interaction. RMON may also be embedded in a product, which allows interconnect devices to serve as monitors.

RMON probes also have some drawbacks. They can't capture and decode packets. Probes can't generate traffic loads for testing and network optimization, either, noted *LAN Times*.

**Protocol analyzers.** Unlike RMON probes, protocol analyzers can capture and decode packets. A few can suggest solutions for problems detected, while others have a proactive feature, generating alerts when predefined thresholds are exceeded. Some can generate loads to simulate real life network traffic.

However, protocol analyzers have several major drawbacks.

"A significant problem with most protocol analyzers is that they can monitor and capture only the packets they see," noted a recent issue of *LAN Times*.

In addition, protocol analyzers are difficult to use, expensive and cumbersome, according to analysts at the Gartner Group, Inc., a Stamford, Conn. based consulting firm. Most lack an intuitive graphical user interface. To be used effectively, they require a skilled network technician. And many companies purchase a single analyzer and then ship it, along with the technician, wherever it's needed, the analysts say.

### Mutual Shortcomings

Since both protocol analyzers and RMON tools use the same basic Ethernet chips as the devices they're monitoring, they are unable to detect faults due to out of spec components, interference and noise. Furthermore, RMON probes and protocol analyzers' inability to provide a view of physical problems on the network leave a partial blind spot in network monitoring. "There is still a lot of room for error with these technologies," says Villars of IDC.

Conventional network monitoring tools have several other weaknesses. They cannot ensure that each network component is running according to specification as the network runs. Therefore, network administrators are not in a position to proactively identify components that are about to fail. Furthermore, conventional tools usually are limited to collecting network and cable performance measurements—they cannot diagnose problems.

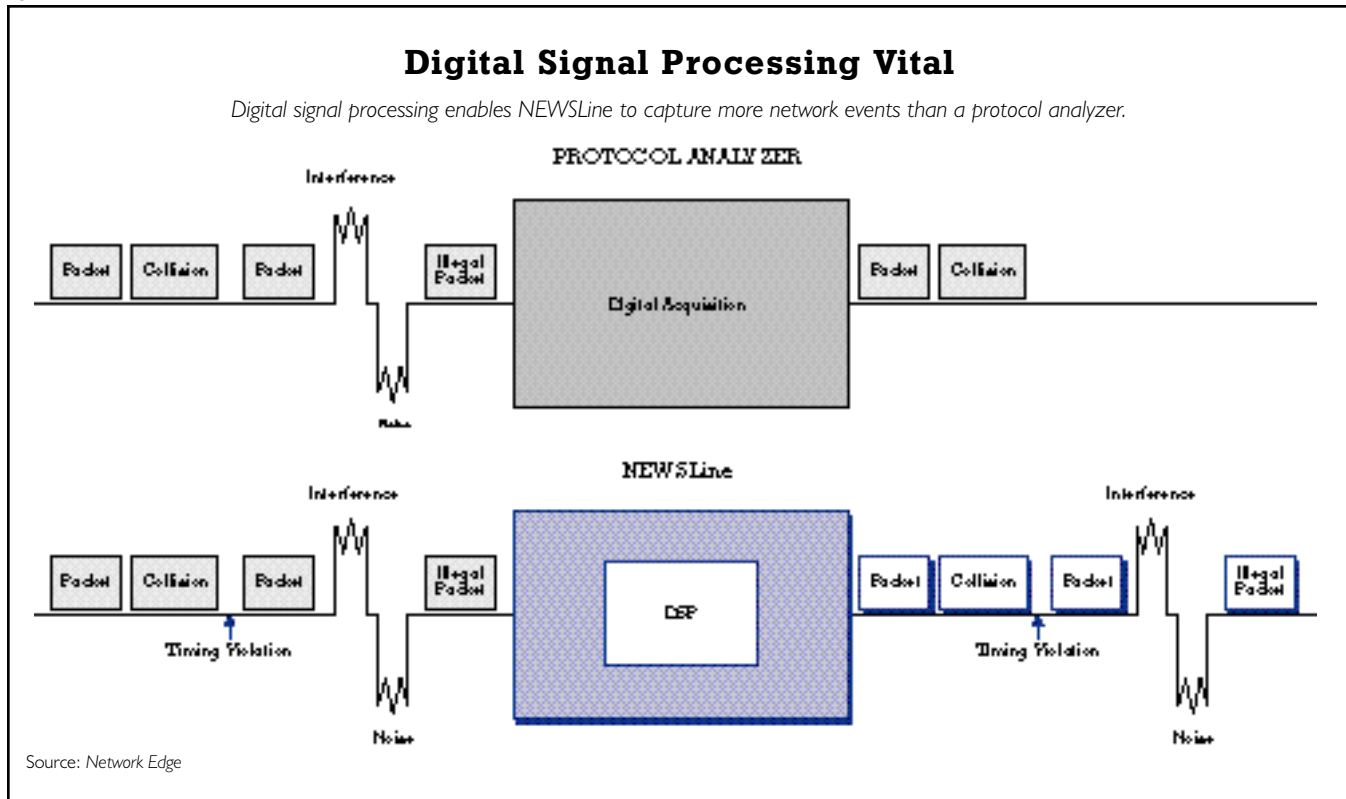
*InfoWorld* test results for several such products concluded that "all of the solutions tested in this comparison did a good job of troubleshooting the problems they were designed to detect. But as we expected, no solution was able to isolate all of the problems possible on today's network."

Since many of these devices cannot be used while the network is running, finding a cable problem might require a network shutdown. Since a shutdown of a mission critical network is unthinkable these days, network managers and users are forced to endure the tedious and time consuming trial and error process of fault discovery. "In a large network, the discovery process alone can take days," says Communications Network Architects' Dzubek.

Wasted time and money are the all-too-frequent result of this ad hoc fault detection process, say network managers. "Today network managers must swap out equipment and guess as the cause of problems on a network," says a network manager at a Silicon Valley company. "The entire debug process can be very mystical and involve voodoo rather than science.

**Today network managers must guess the causes of network problems**

Fig. 8



Network managers use rules of thumb to solve these problems, such as segment the network or buy faster routers, because they cannot find the real problem. That can be costly and time consuming alternative. Furthermore, networks can accumulate hidden problems over time and become unreliable, exhibit poor performance or require high levels of maintenance.”

Such shortcomings weren’t critical when LANs were essentially small workgroups with similar NICs and hubs. Many network managers had installed their networks, and they often intuitively knew the cause of the physical problems and could fix it with minimal downtime. In the current environment where networks are the backbone of the enterprise, network managers need a more powerful and comprehensive solution than current tools.

## An Effective Alternative

The introduction of NEWSLine product family to monitor the physical layer of a network represents a new era in LAN management. It uses digital signal processing (DSP) software to monitor all events on a network with the precision of a laboratory instrument. The state-of-the-art DSP technology enables NEWSLine to detect events missed by conventional

tools (See Fig. 8). “It would be impossible to find these phenomena without NEWSLine,” notes a network manager and beta tester of NEWSLine, who declined to be identified.

With each capture of network events, NEWSLine measures a variety of electrical parameters of a network, including voltage, current, impedance and timing. This enables network managers to view previously undetectable events, including noise, timing violations, illegal packets, spikes, crosstalk and interference from office lighting or elevators.

**“NEWSLine lets us see previously undetected problems in our network”**

“NEWSLine lets us see previously undetected problems in our network, including hub interoperability issues, interference, cabling defects and NIC malfunctions,” says the beta site manager. “Without this product, these problems could not have been detected.”

## Missed Causes

NEWSLine “provides an X-ray of the network at the physical layer,” adds Rick Villars of IDC.

With this information, network managers are able to isolate problems immediately rather than take one to ten hours for trial-

*Other technologies can see the symptoms of the illness but cannot see the cause*

and-error troubleshooting. "Other technologies can see the symptoms of the illness but cannot see the cause," explains the beta site manager. "Only this technology can see the true root of the problem and allow you to address the cause rather than the effect of the problem. This dramatically improves network uptime."

**NEWSLine  
dramatically  
improves  
our network  
uptime**

Furthermore, the NEWSLine technology also tracks the electrical properties of transmitters, cables, and terminators, verifying compliance with EIA/TSB and TSB specifications. In addition, NEWSLine's auto discovery capability provides network managers with the

identity of any network component, such as a hub or a port, as well as pinpoint the location of the device. NEWSLine includes a graphical user interface which displays a network map that includes such identifiers as segment number, port ID number, distance, and source address. Should there be any moves, adds or changes, the network map is automatically updated with the new information. These capabilities allows network managers to identify a field replaceable unit, as NEWSLine differentiates between failures in cable, cable placement, NIC and internetworking devices. The display locates the item without requiring repair personnel to refer to full wiring diagrams.

Fig. 9

<b>One Tool for Many Tasks</b>					
<i>NEWSLine combines the network, fault analysis, indicators, and measurements of a variety of point solutions, including RMON probes, cable meters and protocol analyzers.</i>					
		<b>Type of Equipment</b>			
	<b>Characteristic</b>	<b>NEWSLine</b>	<b>RMON</b>	<b>Protocol Analyzer</b>	<b>Cable Tester</b>
<b>Price</b>	Price per Unit	\$10,000/Server \$5,000/96 Ports	\$5,000/100 Ports	\$20,000- \$40,000	\$5,000
<b>Configuration</b>	Connect Without Interrupting Network (Embedded/Distributed)				
	Portable				
	Handheld				
<b>Cable Test</b>	Test Full Channel Past Wall Plate				
	Automated versus Manual Testing	Automated			Manual
	# of Channels Auto Tested	1997: 24 1998: 384			One
	Bandwidth (MHz)	1997: 165 1998: 400			100-150
<b>Monitoring</b>	SNMP Level Statistics				
	Protocol Decoding of Capture	MAC Level		Full IP	
<b>Conformance Testing</b>	Test Conformance to IEEE/TSB Specs				
	Accurately Identify Source of Non Decodable or CRC Error Transmissions				
<b>Emissions and Noise Testing</b>	Measure Noise and Locate Source				
	Capture and Identify Interference from Lights, Motors, Copiers, etc.				
	Capture and Identify Crosstalk from Other Networks				
<b>Diagnosis</b>	Diagnose Failures Down to Each Discrete Device, Including NICs and Hubs				

Source: Network Edge

Fig. 10

### Beta Site Report

The network manager of a medium-sized West Coast organization was a beta-site tester of NEWSLine. Here is his report:

- Able to see previously undetected problems, including hub interoperability issues, interference and NIC malfunctions
- Now sees "root cause" of network problems, without invoking the "voodoo" of trial and error and guesswork
- NEWSLine pinpoints the problems in networks, greatly improving reliability and productivity
- NEWSLine's graphical user interface reduces the amount of time required to interpret the device's results, relative to other network monitoring technologies

Source: Network Edge

If a packet's source address is corrupt or unavailable, NEWSLine compares the packet signature to a database of "algo-rhythmic fingerprints" to determine the source of the transmission. By contrast, traditional SNMP monitors and protocol analyzers are unable to identify the source of such problems.

NEWSLine also supports passive device monitoring to examine the cable. For example, it enables diagnoses of cross connect, horizontal wiring, wall plates, patch cables, and terminators. In addition, NEWSLine allows automated testing of multiple lines, and tests can be carried out on live networks several times a day without human intervention.

In addition, information stored by NEWSLine can be manipulated in a relational database to generate reports on a number of issues, including throughput, mean time between failures, mean time to repair and percent of uptime and downtime. ■

**NEWSLine allows automated testing of multiple lines, and on live networks**

## Bibliography

### Periodicals

Baird, Wayne C., "Network ghostbusting with hand-held analyzers," *Network Computing*, July 5, 1996

Bisbee, Frank, "Level-The New Standard," *Cabling Business*, ([www.anixter.com/about/news/x3268100.htm](http://www.anixter.com/about/news/x3268100.htm))

"Bottleneck Busters: Stop Network Bottlenecks Before They Happen," *InfoWorld*, April 10, 1995

Buerger, Dave, "Category 5 Users Face Hidden Speed Bumps," *Network World*, August 4, 1997

Caruso, Jeff, "Overcoming UTP Limits," *Communications Week*, April 14, 1997

Chae, Lee, "Lesson 93: Cable Testing," *LAN Magazine*, May 1, 1996

Edwards, Brad, "Keep Traffic Flowing," *LAN Times Online*, June, 1997

Geier, Jim, "Reading the cable meter," *LAN Magazine*, August 1, 1996

Greenfield, David, "Wire Act Leaves LANs Dangling," *Data Communications*, February, 1996

Larsen, Amy, "Stackable Hubs: Frills Without the Bills," *Data Communications*, April, 1996

Lazar, Gerald, "The Rise Of Integrationware," *Information Week*, May 5, 1997

Metcalfe, Robert M., "Ethernet Elders Confirm the Chip Bug Scandal," *InfoWorld*, March 14, 1994

"Network Troubleshooting," *InfoWorld*, April 9, 1997

"External Noise," Chuck Siebuhr, *Cabling Business*, March, 1997

### White Papers

"Balance and the Media Twist Performance Advantage," Anixter, Anixter Online Technical Library, 1997 ([www.anixter.com/techlib/vendor/cabling/x3213100.htm](http://www.anixter.com/techlib/vendor/cabling/x3213100.htm))

"Category 5: How Did We Get Here and Where Do We Go Next?" Jim Serenbetz and Pete Lockhart, Anixter Inc., Anixter

Online Technical Library, 1997 ([www.anixter.com/techlib/whiteppr/cabling/x4156102.htm](http://www.anixter.com/techlib/whiteppr/cabling/x4156102.htm))

"The Direction of the Corporate LAN," Vince Magno, Lucent Technologies, 1997 ([www.anixter.com/techlib/vendor/cabling/corpnet.htm](http://www.anixter.com/techlib/vendor/cabling/corpnet.htm))

"UTP vs. STP: A Comparison of Cables, Systems, and Performance Carrying High-Data Rate Signals," Lucent Technologies, Anixter Online Technical Library, 1997 ([www.anixter.com/techlib/vendor/cabling/att/UTP.htm#vs3](http://www.anixter.com/techlib/vendor/cabling/att/UTP.htm#vs3))

### Books

Saunders, Stephen, *The McGraw-Hill High-Speed LANs Handbook*, New York, McGraw Hill, 1996

## About This Report

*Network Edge* is a report that synthesizes analysts' research on various networking topics for network operators at large and medium-sized organizations around the world. It is published by the Network Products Division of LeCroy Corp. to help network operators better manage their systems.

This edition of *Network Edge* is based on interviews and documents from a variety of consulting firms and market research organizations. The authors gratefully acknowledge the cooperation of Communications Network Architects, Dataquest, Gartner Group, Infonetics Research, In-Stat, International Data Corp., NetWare Research, Northeast Consulting Resources, Optimized Engineering Corp., Sage Research, Sentry Research and Analyst Services and the Tolly Group.

## About The Authors

Lee Sustar is a freelance writer based in Chicago who has specialized in networking and information systems for more than 15 years. He has contributed to such publications as *CommunicationsWeek*, *Computerworld*, and *PC Week*. In addition, Sustar has written reports and other technical writing projects for IBM, Digital Equipment Corp. and AT&T.

Larry Marion is the publisher and editor-in-chief of *Network Edge*. He has more than 20 years of experience as an editor, writer and analyst on various information technology subjects. Marion has produced reports for the Business Research Group, Cambridge Technology Group, and Price Waterhouse. His articles have appeared in *Computerworld*, *Datamation*, *Information Week*, *PC Week*, and *Software Magazine*.

## For More Information

For more information about NEWSLine please contact the Network Products Division of LeCroy: 888-654-NEWS (6397) or visit the LeCroy website, [www.lecroy.com](http://www.lecroy.com). Fax: inquiries to 781-270-9414 or write to Network Products Division, LeCroy Corp., 25 Burlington Mall Rd., Burlington, MA 01803

## Network *Edge*

### Publisher/Editor-in-chief

Larry Marion

### Editors

Elizabeth Lindholm

Arlene Richman

Chris Staiti

Lauren Paul

### Analysts/writers

Gerald Lazar

Emily Kay

Dan Orzech

Alan Radding

Teri Robinson

Lee Sustar

### Designer

Mary Avery

Carlson Webster Avery

Westport, Mass.

### Subscription information

For additional copies of this report, permission to reprint or excerpt it, or to distribute it electronically, please contact the Network Products Division of LeCroy:

Telephone Number: 888-654-6397

Fax: 781-270-9414

USPS: Network Products Division,  
LeCroy Corp., 25 Burlington Mall Rd  
Burlington, MA 01803

E-mail: [NEWSLine.sales@lecroy.com](mailto:NEWSLine.sales@lecroy.com)

Editorial support provided by  
Competitive Edge Information Services, Inc.  
of Newton, MA

---

Network Products Division  
LeCroy Corp.  
25 Burlington Mall Rd.  
Burlington, MA 01803