LAN Diagnostic Devices: The Market, Products, and Vendors

In this report:

Editor's Note

This report provides information on LAN diagnostic device market leaders and market trends; details the features and capabilities of several significant LAN protocol analyzers; describes other LAN diagnostic devices types; and includes the addresses and telephone numbers of the leading LAN diagnostic device vendors.

Report Highlights

LANs fail for many reasons. Broken or intermittent hardware, software bugs, and improper configurations are among the more frequent causes. If your LAN fails, you will feel more confident when you have the necessary equipment to help you get to the root of the problem. LAN protocol analyzers provide a variety of functions necessary for testing, analyzing, and evaluating LAN faults and their causes. Lower cost diagnostic devices are also available for monitoring simple LAN configurations or as additional tools in the problem-solving kit. The LAN diagnostic devices discussed in this report represent a significant cross section of the types available today.

This report was developed exclusively for Datapro by Arnold S. Cleff. Mr. Cleff is an independent communications consultant and free-lance writer. He has developed software and hardware for test equipment, process control, energy management systems, data communications, and network management systems. He was formerly Director of Systems Engineering for Digilog and Manager of Systems Software for Leeds and Northrup.

Market Leaders

The firmly entrenched leader in the LAN diagnostic market remains Network General. The company provides a case study in organizing and carrying out an attack on a marketplace. Other vendors, nonetheless, are competing vigorously to catch up and stake their claims to a larger share of the action.

Among this group are:

- Novell/Excelan (newly united in 1989 to diversify their LAN offerings);
- Spider Systems (with an array of LAN monitors and protocol analyzers);
- Hewlett-Packard (the market leader in the WAN protocol analyzer market);
- Racal InterLan (another 1989 merger, offering a plug-in protocol analyzer for IBM-compatible ATs); and
- Digilog (also a vendor in the WAN protocol analyzer market, recently acquired by CXR, and entering the LAN arena with an

interesting combination of standalone and system-oriented diagnostic equipment).

The competition further heats up with M-Test Equipment, introducing a 1990 entry that provides a first in LAN diagnostics—auto diagnosis. Other key players include AR Division of Telenex, also a WAN protocol analyzer vendor, and International Data Sciences (IDS), offering a combination LAN/WAN package. Prodatel and Performance Technology provide unique offerings to special segments of the LAN market.

Market Trends

Mergers and acquisitions continue to be a key market trend. Increased network complexity and interoperability is another. The two are related, since the need to deal with complexity drives companies to merge their resources and talents to offer more complete, competitive answers. The design and functionality of diagnostic devices are traditionally driven by this problem. To better understand where these devices are going, let us have a quick look at the problem(s).

With the LAN market reaching out to provide more sophisticated operating systems, more powerful and intelligent devices for connectivity, faster workstations, and the capability to span any distance, the problem becomes one of dealing with increasingly complex networks. The LAN gains more devices, is extended with more bridges and routers, and adds more interconnections to other LANs. Interconnected LANs may employ diverse operating systems that in turn may employ different protocols. Other manifestations of maintenance complexity accrue when copper and fiber optic cable are configured within the boundaries of a LAN or network of interconnected LANs or when a wide area network or a private network spans between two LANs.

LAN diagnostic device vendors must deal with these trends by building the capability into their products to handle more variations while at the same time simplifying its operation and maintaining price competitiveness. Solutions to these problems appear in many forms. A full-power protocol analyzer on a plug-in card for IBM PC-compatible computers is a low-cost solution. A low-power, low-cost analyzer on a plug-in card is a variation of this approach. For remote monitoring on larger LANs, special remote or slave units, working in conjunction with a master protocol analyzer or network management system, are available. These remote devices typically offer a low-cost method to distribute protocol analysis capability through the network and at the same time permit control and review of remote data from a central site.

To service the many network configurations and protocols, the most powerful analyzer must have the capacity and capability for field expansion, to interface to almost any type of LAN architecture, protocol, or operating system. Seemingly limitless capability can be purchased, but it is costly. To meet the challenge of developing products that interface to the variety of architectures and speeds, devices, and uses of the LAN while providing increased functional flexibility, LAN diagnostic vendors offer add-on software modules.

Common Features of Protocol Analyzers

The following paragraphs summarize the features most frequently found in LAN protocol analyzers. Differences in method of implementation and degree of functionality, for both hardware and software, distinguish one product from another. These differences, at times subtle, vary in importance with users and their networks. No product is equipped with all features, making it difficult to decide which product is best for a given user.

User Interface

Menu-driven systems, interactive user input, graphics- and character-oriented output displays, and function key control are standard features, with quantity, quality, and presentation formats differing for each product.

Some common display features are:

- frame-oriented sequence for traffic flow;
- single station-for-station analysis;
- two-station analysis for a command/response context;
- network for overall statistics and performance;
- alarms/events log to track problems or conditions;

- protocol decodes by single layer or multilayer to interpret message content;
- split-screen, either side by side or one over the other; and
- windowing, both built into the vendor software and external through packages such as Microsoft Windows.

Capture Buffers

Capture buffers vary in size and may be embedded in a plug-in card or be part of the host PC RAM. Embedded capture buffers permit design control over memory bus architectures and bus speeds and can contribute to a higher level of performance when capturing data, but those features can be at the expense of capture buffer size. Capture buffer size determines the device's capability to capture all relevant data from the network for playback and analysis. When the data streams in faster than it can be captured, information loss occurs—an unacceptable situation. Manufacturers go to great lengths to avoid this condition.

Eventually, however, any size capture buffer will fill. Then, two techniques are employed—automatically stop the capture or wrap around (overwrite) to the start of the buffer.

Filtering

Filters applied to incoming data limit the capture of data to those frames that meet the filter criteria. This saves valuable capture buffer storage and eliminates the need to review unwanted frames. Filters vary in quantity, size, and where and how they can be applied against the incoming data in the frame. Additionally, some analyzers allow post-filtering, a process that filters data from the capture buffer during playback and review.

Filters help in several ways. They reduce the quantity of captured information, thus preserving valuable capture buffer storage space. With a judicious filter applied against the incoming information, only relevant data need be reviewed, which speeds and simplifies the review process. The obvious question is, if you do not know the problem, what filter criteria do you use? Experience is one answer; trial and error is another.

Triggers

Triggers are mechanisms that start or stop the capture of data. Common triggers are manual start/stop, time of day, relative timing, and contents of the frame. Triggers can be used in conjunction with filters to further refine the content and quantity of capture buffer data. This technique refines the analysis process, too, limiting the capture to the essential information necessary to reveal the problem source. Once again, experience, coupled with a little luck, often prevails. Of course, triggers can be used in another context—to provide sampling, based on time of day or other criteria, for historical purposes. The more sophisticated the trigger mechanism, the more powerful the function.

Search

Some protocol analyzers provide a method to search through the capture buffer to locate specific information for replay. While a filter searches for a given condition and then captures or displays only the information meeting the criteria, the search function reviews the information already in the capture buffer and locates that which meets the search criteria. This function eliminates having to manually view the full contents. As with a trigger, the more sophisticated the search criteria, the more useful the technique.

Time Stamping

Incoming frames are individually time-stamped to aid in the analysis of network performance. The time stamp resolution varies from a microsecond to tens of microseconds and is influenced by equipment design criteria versus the speed of the LAN. Among the uses for time stamping is the analysis of actual network timing versus specified network timing. Keep in mind that time stamping is applied by the diagnostic device and not the normal network application element or server. Nonetheless, it can be used in a variety of ways to test network performance.

Traffic Generators

Traffic generators force loads onto the LAN to determine its reaction and resiliency, thereby previewing how the LAN will react before such conditions actually occur. Traffic generators vary in the quantity of channels of information they will transmit, channel information content, frequency of transmission, and control over other attributes pertinent to transmission of frames on a given network physical media. They are excellent tools for both preventive and reactive analysis.

Ethernet Cable Checks

A built-in time domain reflectometer (TDR) tests the cable for faults. This can be performed automatically upon start-up of the analyzer or manually.

Symbolic Station Names

Naming stations is a database facility that permits the user to enter manually a symbolic name for a given station address. It permits the system to substitute a more readily recognizable symbol in place of the station number in its station-oriented displays.

Self-Test Diagnostics

A self-test is performed on power up and possibly (but not likely) upon other conditions. Self-test is useful when there is a need to troubleshoot the diagnostic device itself. Understanding the purpose and extent of each self-test and establishing confidence in its thoroughness is helpful; however, self-tests are rarely, if ever, a criterion for product selection.

Hard Copy Printing

Most analyzers permit printing of various displays and information. This feature varies considerably in its implementation among vendors and their products. Hard copy printing can offer a simple output of the screen or be considerably more sophisticated in the handling, formatting, and printing of capture buffer information. It is more convenient to specify criteria and have the system search the capture buffer to locate the required information and automatically format and print it than to manually bring up each screen and request that it be printed. You should look carefully at how this feature is implemented in your favorite analyzer, to determine if it meets your needs. Hard copy output is handy for distributing or faxing conditions to others for group analysis and for historical record keeping.

Password Protection

Since protocol analyzers can display complete frame contents, security may be a concern. For these instances, limited access via password protection is useful. Varying degrees of security are provided in protocol analyzers. If this is a significant concern (for example, at a financial institution), check the controls and robustness of the protective procedures.

Protocol Analyzers

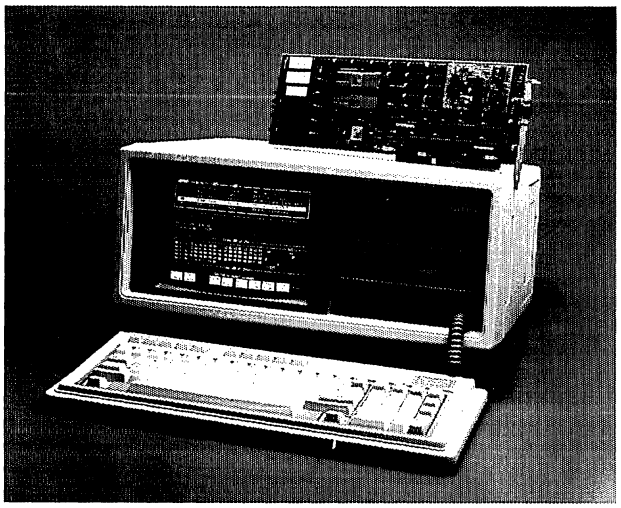
The following overviews of representative protocol analyzers provide insight into their features and functionality. They are not intended to be, nor should they be used as, a direct comparison to evaluate one model against another. Selected features are presented to provide an overview of a product and do not include all of that product's features and capabilities.

The Sniffer (Network General)

The Sniffer offers plug-in hardware to interface to an extensive selection of LAN physical media, including IBM Token-Ring (4M-byte and 16M-byte versions), Ethernet, IBM PC Network (Broadband), ARCnet, Starlan, and LocalTalk. The Sniffer has software modules that support a broad set of protocols suites for IBM, Novell NetWare, XNS/MS-Net, TCP/IP, SunNFS, ISO, DECnet, Nestar PLAN, Banyan VINES, AppleTalk, and X-Windows. A typical user is likely to need only a subset of these options to maintain even a large and complex LAN.

The base unit includes one network interface module and software for menuing, capture, analysis, display control, and protocol decoding of the appropriate lower layers. Optional protocol interpreter software modules are available for higher layer decoding of the various packet protocols. Network General provides the user with the flexibility to initially configure The Sniffer to meet current LAN needs and to upgrade it as the LAN changes.

Adding to its versatility, The Sniffer operates on two equipment platforms. The 300 Series uses an 80286-based processor with a standard 3M-byte RAM capture buffer; the 500 Series uses an 80386-based processor with an optional 8M-byte RAM capture buffer. The 500 Series Sniffer is installed in a Compaq Portable 386, and the 300 Series Sniffer is installed in a Toshiba 3200. Users can purchase the plug-in hardware and software as a separate package to install in their own Compaq Portable 386. The software is not sold separately. If



The Sniffer, from Network General, is the most popular LAN diagnostic device on the market today. The Sniffer provides diagnostic capabilities for Ethernet, token-ring, ARCnet, IBM PC Network, Starlan, and LocalTalk LANs.

you support more than one type of LAN, the Compaq version can be optionally configured to interface to multiple LAN physical media.

Network General recently introduced a software package, SniffMaster I, to run with Sun Microsystems' SunNet Manager. In this configuration the user can monitor and control Sniffer analyzers located in both local and remote segments of the LAN.

The Sniffer supports time domain reflectometry (TDR) for locating cable breaks in Ethernet configurations, a feature found in some, but not all, LAN protocol analyzers. The Sniffer also has a traffic generation feature to load the network with frames of selectable sizes to calibrate performance under stress conditions. The standard software module provides remote control of The Sniffer from any IBM-compatible PC, using a modem connection over the RS-232 serial port.

Frames can be captured based on selectable filters, to reduce the quantity of information stored per frame in the capture buffer. These include combinations of truncating the frame to the first 32, 64, 128, 256, or 512 bytes; matching source/destination pairs; low-level protocol content; pattern matching; frame errors; or destination class. Other features include capture triggers, stop capture parameters, and time-stamping of frames.

In general, The Sniffer frame display and analysis includes a summary view of the frame content, a detail view for each frame in English or hexadecimal, windowing capability with zoom or scrolling, and other significant functionality. Greater functionality often requires more user skill to take full advantage of available information content. The Sniffer provides a variety of display types with presentations in both graphics and character format. The full set of displays and their content are beyond the scope of this summary and will vary as a function of the LAN physical media and the LAN protocol.

A general overview of display options includes graphics skyline displays simultaneously showing network frame count and active stations per unit of time and bar graphs displaying traffic density in terms of frames per second, kilobytes per second, or percent of bandwidth. Character displays provide information on node activity based on individual station selection or two-station selection showing a command/response sequence. There are also network summary displays on a frame-by-frame sequence. Information content includes packet timing, destination, source, and other decoded frame fields. Displays can be shown live or replayed from the capture buffer.

A key feature of The Sniffer is the degree of decoding provided at each of the protocol layers and the options available to selectively display this information. If this is not sufficient, user-defined protocol interpreters can be written in C language and deployed with Sniffer-provided library routines.

No vendor offering can have everything; i.e., a superset of all features provided by every manufacturer. Consequently, a feature of key importance for a particular environment may not be available on The Sniffer. The Sniffer does have a wide variety of features and capabilities; in fact, it may offer more than the user needs or may be too expensive. It is, however, probably the most powerful and sophisticated product available.

LANalyzer (Novell/Excelan)

Excelan, now Novell's LANalyzer Product Division, offers alternative choices for LAN diagnostic device users. The LANalyzer provides a protocol application library for extensive analysis in the lower four or five OSI protocol layers, areas that Excelan considers to be key in uncovering problems related to managing a network. Novell has also introduced a companion product, LANtern,

an Ethernet network monitor employing the Simple Network Management Protocol (SNMP) to communicate over the network from its remote location to a network manager's console. In terms of managing the network, Excelan views the three upper layers to be associated more with the needs of software engineers writing network applications. When necessary, access to these layers can be gained by the network administrator through interfaces in relevant applications programs. Focusing on where the majority of problems occur, the LANtern targets the lower three OSI protocol layers.

The LANalyzer interfaces to a variety of network physical media with plug-in analyzer boards for Ethernet (EXOS 325) and token-ring (EXOS 325TR) and an optional Starlan adapter for the Ethernet board. The LANalyzer software library provides modules for AppleTalk, TCP/IP, NFS, OSI, RFC 1001- and 1002-compliant NETBIOS, SUN RPC packets, SMB functions, XNS packets, and Yellow Pages.

LANalyzer can be purchased as a complete package, including a NEC PowerMate Portable SX platform and one or more plug-in analyzer boards, or the plug-in analyzer boards can be purchased separately and inserted into the user's IBM-compatible PC AT. Each board requires its own expansion slot, including the Starlan adapter for the Ethernet version. The board package includes the LANalyzer software application library.

The Ethernet version of LANalyzer provides cable checks. Both the Ethernet and token-ring versions generate network traffic to stress test the network under various conditions, according to the specific physical media characteristics. On Ethernet, for example, varieties of control include frame sizing, multiple transmit channels (six maximum), selectable interpacket delay times, packets with CRC errors, and collision generation.

LANalyzer employs a special controller design to detect events that a standard LAN controller may ignore. It also uses on-board memory to store data through its own bus, rather than depend on the speed of a host system bus. This capability may prove relevant for future product upgrades as LAN transmission rates continue to increase and fiber optic cabling becomes more commonplace.

LANalyzer has a menu-driven user interface with displays presenting realtime capture and display, as well as off-line search of the capture buffer. Display formats have both graphics and character orientation. LANalyzer also provides time stamping of incoming data and capture buffer triggering and filtering. Realtime statistics for Ethernet include collision counts, CRC/align errors, short packets, utilization, and filtered counters. Realtime statistics for token-ring include MAC frames, ring recoveries, token rotation time, utilization, and filtered counts. LANalyzer also prints realtime statistics at selectable time intervals.

LANtern

LANtern is a LAN network monitor. Designed for remote installation, it monitors and transmits information to a central site, providing diagnostic information for the management of a large LAN. LANtern sends its data over the network using the SNMP protocol. It can traverse network segments and, conversely, be controlled from the central site. An important use for this type of device is unattended network monitoring and status and early warning of deteriorating network conditions. This information enables proactive or reactive maintenance, including (if necessary) a visit to the remote location by personnel equipped with additional diagnostic devices to further evaluate the situation and resolve the problem.

Comtest LAN Analyzer (M-Test Equipment)

The Comtest LAN Analyzer, a 1990 newcomer, appeals to the LAN manager who wants the analyzer to do more than present information. M-Test Equipment touts, for those who expect the analyzer to analyze, the Comtest LAN Analyzer auto diagnose screen. Using a single key (F2), the Comtest LAN Analyzer executes a full diagnostic check of the network, including TDR. The Comtest LAN Analyzer displays all found faults, with a supporting list of symptoms, leading to the screen display of the problem's cause. In addition, each fault is given a level of severity grade, noted by asterisks. For example:

- *=suspected error—single node problem
- **=confirmed error—1- or 2-node problem
- ***=suspected error—major component problem
- ****=confirmed error—major component problem
- *****=a network-wide problem—e.g., a segment down

Displaying the fault, its severity grade, and the list of associated symptoms on the auto diagnose screen, the Comtest LAN Analyzer simplifies the diagnostic process.

Comtest LAN Analyzer interfaces to Ethernet network physical media and installs in an IBM-compatible PC. It offers a full set of features and capabilities. Protocol decodes are available for OSI-LLC1, LLC2, X224, X225, TCP/IP, XNS, IPX, SPX, X.25, SNA, DECnet, Novell NetWare, Banyan VINES, and Sun RPC. Other Comtest LAN Analyzer features include filters, 4M-byte capture buffer, time stamping, data logging to disk, alarm and events log, TDR, support for graphics and color printers, menu-driven user interface with split screen and windowing, password protection, traffic generation, and optional remote control.

LANVista (Digilog)

Digilog's initial offering in the LAN market, LANVista, is more than a LAN protocol analyzer. Offering the choice of an integrated package on an IBM-compatible PC platform, a plug-in LAN protocol analyzer, or remote slave units, the system competes with other vendors' offerings in a number of ways. LANVista interfaces to Ethernet and IEEE 802.3 network physical media; a planned option will interface to token-ring.

In addition to standalone protocol analysis, LANVista offers versatility in the placement of its master PC console and the slave units.

The master PC may be:

- the integrated package from Digilog;
- the user's PC with a plug-in slave board; or
- the user's PC interfaced to the LAN by a master Interface card and serviced through the LAN by a slave unit added to the LAN.

The slave units can be located in any LAN segment. In addition, the master PC can be serviced by a remote slave unit over a modem connection between the slave unit and the master PC serial port. LANVista software executes in the master PC in all of the above variations and can handle multiple slave units. In combination with Microsoft Windows, it can communicate with different slave units at the same time. LANVista software is intended to decode all seven layers of popular LAN protocols.

LANVista tests cables using built-in TDR. The slave units also have TDR capability and, under control from the master PC, perform these tests at their various remote locations and display the results at the master console.

LANVista can generate network traffic to stress the system and calibrate the results. It provides for variations in traffic generation format including percent loading, quantity and size of frames, frame content, and frame gaps.

The product offers a variety of displays in both graphics and character formats. Display types include full seven-layer decode, single-layer decode, network utilization, LAN segment statistics, frame gap distribution, and frame length distribution. LANVista also provides time stamping of frames, capture buffer filtering, frame slicing to reduce the quantity of information stored per frame, and triggers. Multiple capture buffers can be stored on hard disk.

LANVista's flexible hardware configurations allow it to diagnose basic or complex networks.

HP 4972A LAN (Hewlett-Packard)

Hewlett-Packard, the leader in WAN protocol analyzers, offers the HP 4972A LAN to interface to Ethernet, IEEE 802.3, and (optionally) Starlan network physical media. The HP 4972A LAN provides Layer 2 protocol analysis for Ethernet; IEEE 802.3/Starlan; and optional multilayer protocol analysis for XNS, DECnet, TCP/IP, and SunNFS. Interestingly, the HP 4972A LAN is designed on an HP platform, not on the IBM-compatible PC platform used by many other vendors in the LAN protocol analyzer market. This permits HP extra design flexibility in its architecture to emphasize any areas it considers essential.

The HP 4972A LAN includes a 1M-byte capture buffer, hard disk and diskette storage, logging of data directly to disk, timers to regulate events, counters to track events, and time stamping of incoming frames. It also provides for traffic generation of up to 16 messages of selectable length, content, and transmission rate. An optional remote interface to control the device from a central location is available.

Data is presented through a variety of displays, including network summary, collisions versus time, network utilization versus time, frame

length versus time, node traffic, and many other performance-critical displays plus protocol-specific decodes.

Interview 1000 (AR Division of Telenex)

The Interview 1000, from the AR Division of Telenex (formerly Atlantic Research), is a full-power token-ring and Ethernet LAN protocol analyzer consisting of a base unit with detachable monitor and keyboard. It provides an array of features for monitoring, analysis, and traffic generation. The Interview 1000 includes filtering, event analysis, timing relationships, and full-duplex operation to emulate a station and simultaneously capture and display data. The Interview 1000 has a menu-driven user interface with a versatile set of presentation displays.

The base unit includes a 40M-byte hard disk, 2M-byte diskette, 80286 microprocessor, bit-slice network preselector, and VMEbus architecture. It is a self-contained unit, designed more along the line of traditional WAN protocol analyzers. Its special architecture provides more control over performance and design flexibility than a plug-in board in an IBM-compatible PC.

Sherlock LW (International Data Sciences)

The Sherlock LW from International Data Sciences (IDS) is a LAN/WAN protocol analyzer in a laptop computer. It can be outfitted to handle Ethernet, token-ring, and any WAN in a NEC 286 Portable PC package. This report summarizes only the LAN aspects; the WAN features are also impressive.

The Sherlock LW has optional software decodes for Ethernet and token-ring protocols. The Ethernet list includes DECnet, Novell, TCP/IP, SUN, ISO, AppleTalk, and Banyan VINES protocols up to Layer 7. The token-ring Layer 7 decodes include Novell, TCP/IP, ISO, NETBIOS, and SNA (TBA).

Sherlock LW operates under menu control with password protection and presents data in various formats including graphics- and character-oriented displays. Display information includes peak and average network utilization, network activity, and network loading. Statistics available include information such as collisions, short packets, packets sent, packets received, bytes sent, bytes received, and error rate. A special feature permits preset conditions to alert the user to the alarm condition.

TDR testing and traffic generation are provided. The device also has capture buffer filters and stores capture data in RAM or on hard disk. Remote monitoring between units is possible.

SpiderMonitor/SpiderAnalyzer (Spider Systems)

SpiderMonitor 220 and the SpiderAnalyzer 320, from Spider Systems, are LAN protocol analysis devices designed for use by the LAN manager and the LAN developer, respectively. SpiderAnalyzer extends packet analysis to suit the developer's frequent need for extreme detail. Both units interface to Ethernet and IEEE 802.3 network physical media and are menu driven, with a full set of display screens formatted for LAN analysis presentation. Both come in an integrated package housed in a Compaq Portable III or in kit form for plug-in to IBM-compatible PCs. Both operate in various operational modes including alarms, performance, development, statistics, summary, TDR cable test, and traffic generation. Spider software packages handle protocols such as SNMP, ISO, DECnet, TCP/IP, and XNS.

LAN Detector (Racal InterLan)

Racal InterLan's LAN Detector is a plug-in LAN protocol analyzer for IBM-compatible PC ATs. Racal InterLan offers an array of solutions for providing LAN interconnections; LAN Detector plays one part in the overall picture. LAN Detector interfaces to Ethernet and IEEE 802.3 network physical media. It supports protocols including Novell, XNS, TCP/IP, SUN PC-NFS, OSI, Banyan VINES, AppleTalk, and DECnet.

LAN Detector has built-in TDR for locating cable faults. It can also generate network traffic to stress the network for determining performance under load. It is menu driven for user access to displays, control selection, and data entry. Help is available through the keyboard for information on specific topics. It provides remote diagnostic capability via modem connection to a PC with an installed LAN Detector. Data can be printed for hard copy analysis or stored on disk in ASCII format for later retrieval.

Filters capture live data from the LAN and store it in the capture buffer. Captured data can be viewed on-line or replayed later. Displays with various formats present data in either graphics or character mode. Information displayed includes

peak activity, traffic patterns, overall network activity, and network utilization. Timing information is shown as time between successive frames, time relative to a specific frame, and absolute time of day. Protocol decodes display information in English or in hexadecimal formats.

Prodatest IV (Prodatel Communications)

Prodatel offers the Prodatest IV, packaged in an IBM-PC compatible platform, as a low-cost protocol analyzer for Ethernet, IEEE 802.3, and Starlan LANs. It provides traffic generation, simulation, and capture of filtered LAN traffic. The Prodatest IV is menu driven, and its various displays present both live or captured data, in either frame format or statistical format.

The software package included with the Prodatest IV features an Intelligent-Symbolic Packets Interpretation (I-SPI) mode that permits the user to view and interpret each field in a frame and TCP/IP Layers 3 and 4. Prodatest IV also has a special generation feature for defining triggers and using them to transmit messages in a programmed scenario. With this feature, scripts of varying nature can be generated to test the LAN.

POWERscope (Performance Technology)

Performance Technology's POWERscope is a relatively low-cost plug-in board with software for analyzing ARCnet LANs. ARCnet, a token-passing bus technology introduced in 1977, has a large installed base, though it has yet to be standardized by the IEEE 802.3 committee. ARCnet's token-passing bus structure offers an alternative for factory LAN systems requiring token-passing capability.

POWERscope captures selected messages and displays data for review. Captured messages are from specified nodes. The POWERscope package includes a specially modified Resource Interface Module (RIM) board to interface to the ARCnet network physical media, ARCscope software, and a second software module called BIN2ASC that converts the captured ARCnet message file into a more understandable format. Two other software packages are also available: NB Scope for capturing and analyzing NETBIOS packets and SMB Scope for capturing and analyzing SMB packets between workstations and servers.

Other Types of Diagnostic Devices

Oscilloscopes

Oscilloscopes are workhorses for many applications in which signal observation and measurement is essential. They can also monitor and measure signal characteristics on LANs. There are many brands and models, including those from well-known manufacturers such as Hewlett-Packard and Tektronix.

Time Domain Reflectometers (TDRs)

A time domain reflectometer is often featured within an Ethernet protocol analyzer, but several varieties of standalone units are also available. The TDR generates a signal that travels the Ethernet cable and reflects back when cable faults exist. The pattern of the reflected wave reveals the type of fault—short, break, impedance mismatch, etc.—and the distance from the fault to the TDR. Tektronix' Model 1503B TDR includes a front-panel oscilloscope-type display to show the reflected waveform, plus a strip chart record for convenient historical records.

Cable Activity Testers

Datacom Technologies' LANcat 1200 permits several cable tests to be performed on an Ethernet LAN. The LANcat, a handheld device, has LED indicators to note conditions such as jabber, collisions, data present, and cable faults—near shorts (within an inch), shorts greater than an inch, and cable impedance mismatch. The LANcat can also generate a TDR signal and view the results on an oscilloscope. Other features include an LED to indicate the presence of a beacon signal, generated by an accessory device, to detect physical continuity between nodes.

Cable Tracers

The Cable Sender/Tracer from MicroTest provides a method to locate existing cables tucked neatly (or not so neatly) away in ducts, behind walls, etc. When the sending unit transmits on the cable, the receiving unit is moved in the general direction of the suspected cable path until the receiving indicator light signals proximity. Constraints are the maximum distances of the transmitted signal from the sender unit (1,000 feet) and the maximum sensitivity distance from the hidden cable (1 foot) for the tracer unit.

Vendors

For your convenience, listed below are the addresses and telephone numbers of the vendors whose products are discussed in this report.

AR Division of Telenex
7401 Boston Boulevard
Springfield, VA 22153 (703) 644-9190

Datacom Technologies Inc.
11001 31st Place W.
Everett, WA 98204 (206) 355-0590

Digilog, Inc.
1370 Welsh Road
Montgomeryville, PA 18936 (215) 628-4530, (800) DIGILOG

Hewlett-Packard Co.
Business Computing Systems
19091 Pruneridge Avenue
Cupertino, CA 95014 (800) 752-0900

International Data Sciences, Inc.
7 Wellington Road
Lincoln, RI 02865 (401) 333-6200

M-Test Equipment
Box 460008
San Francisco, CA 94146 (415) 861-2382, (800) 334-4293

MicroTest
3519 E. Shea #134
Phoenix, AZ 85028 (800) 526-9675

Novell, Inc.
LANalyzer Products Div.
2180 Fortune Drive
San Jose, CA 95131 (408) 434-2300

Network General Corp.
1945A Charleston Road
Mountain View, CA 94043 (415) 965-1800, (800) 952-6300

Performance Technology
800 Lincoln Center, 7800 IH 10 W.
San Antonio, TX 78230 (512) 349-2000

Prodatel Communications Inc.
720 Montgolfier
Laval, PQ, Canada H7W 4Z2 (514) 686-0232

Racal InterLan
155 Swanson Road
Boxborough, MA 01719 (508) 263-9929, (800) LAN-TALK

Spider Systems, Inc.
12 New England Executive Park
Burlington, MA 01803 (617) 270-3510

Tektronix, Inc.
205 Ravendale Drive
Mountain View, CA 94043 (415) 967-5400 ■