Handy Tools For LAN Managers

Local Area Networks (LANs) are proving an attractive solution to today's organisational information systems. And standardization of LANs now enables users not to be locked into a single vendor but seek heterogonous sets of systems. Debasis Basu and Girish Palshikar look into the emerging trends in managing LANs and details a LAN analyzer as a powerful tool in the hands of network managers.

Since the advent of microprocessors, computers are rapidly becoming smaller, cheaper and more powerful. Hence the media ('computer networking') is an increasingly attractive solution to today's complex organizational and information sharing problems.

Local area networks (LANs) are usually spread over a small area such as an office complex, a business house or an institution and use fast communication media like coaxial or fibre optic cables. LANs usually are based on a regular interconnection topology such as a tree or a ring. The services available on a LAN include sharing of resources like laser printers, file transfer, electronic mail, remote log-in, file servers and the like.

The LAN Technology
The LAN hardware consists of the physical communication medium, network access units, communication control hardware and host computers. The LAN software is divided into a set of hierarchical layers, each layer performing specific tasks for the next layer, hiding details of implementation from it. Each layer communicates with the corresponding layer on another host using a predefined "protocol". A protocol specifies rules governing format, timing, sequencing and error control information about exchanges across a particular layer.

The LAN scenario is made complicated by a multitude of existing industry standards for network hardware as well as for protocols of various layers. The standards have given rise to a multi-vendor LAN market. Owing to its small size, a LAN offers the following advantages:
1) High reliability
2) Easy fault isolation and recovery (serviceability)
3) Plug-in easy physical attachment or relocation of nodes
4) Higher speeds
5) Modularity of structure

and configuration of the system
6) Incremental growth as per requirements
7) install download and maintain network software
8) monitor network performance

What is Management Of LANs?
The management of a LAN is a complex and highly responsible job, which has evolved into a new management post called the LAN manager. Like system administrators and database managers in a data processing environment, a LAN manager is the local LAN guru. The responsibilities span a wide range that include:
- identifying critical LAN applications and users
- evaluation and selection of LAN hardware and software products
- network topology and software configuration
- add/delete/replace nodes and users
- troubleshoot network hardware and software problems
- develop LAN related utilities and applications as required
- help in debugging network applications and so on.

Survey of Available LAN Protocol Analyzers

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Network General</th>
<th>Hewlett Packard</th>
<th>Excelan</th>
<th>Spidernet Systems</th>
<th>DigiLog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>SNIFER</td>
<td>HP 4972A</td>
<td>EX 5500</td>
<td>SPIDER MONITOR</td>
<td>LANVISTA</td>
</tr>
<tr>
<td>LANs</td>
<td>Ethernet</td>
<td>Ethernet</td>
<td>Ethernet</td>
<td>Ethernet</td>
<td>Ethernet</td>
</tr>
<tr>
<td></td>
<td>IEEE802.3</td>
<td>IEEE802.3</td>
<td>IEEE802.3</td>
<td>IEEE802.3</td>
<td>IEEE802.3</td>
</tr>
<tr>
<td></td>
<td>Starlan</td>
<td></td>
<td>Starlan</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Token Ring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arcnet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Compaq</td>
<td>Stand-alone</td>
<td></td>
<td></td>
<td>Card For</td>
</tr>
<tr>
<td></td>
<td>Portable PC</td>
<td>unit with</td>
<td></td>
<td></td>
<td>PC AT</td>
</tr>
<tr>
<td></td>
<td>with 8086</td>
<td>68020, 2MB</td>
<td></td>
<td></td>
<td>with 8086</td>
</tr>
<tr>
<td></td>
<td>8 Mbyte RAM,</td>
<td>RAM and 20</td>
<td></td>
<td></td>
<td>640K RAM</td>
</tr>
<tr>
<td></td>
<td>and 40 Mbyte</td>
<td>Mbyte hard</td>
<td></td>
<td></td>
<td>640K RAM</td>
</tr>
<tr>
<td></td>
<td>disk</td>
<td>disk</td>
<td></td>
<td></td>
<td>20 Mbyte</td>
</tr>
<tr>
<td></td>
<td>hard disk</td>
<td>hard disk</td>
<td></td>
<td></td>
<td>hard disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>advised</td>
</tr>
<tr>
<td>Capture</td>
<td>8 Mbyte</td>
<td>1 Mbyte</td>
<td>2 Mbyte</td>
<td>512 Mbyte</td>
<td>1 Mbyte</td>
</tr>
<tr>
<td>Buffer Size</td>
<td>16 of 32 bytes</td>
<td>16 of 60 bytes</td>
<td>16 of 126 bytes</td>
<td>4 of 64 bytes</td>
<td>8 of 2048 bytes each</td>
</tr>
<tr>
<td>Filters and</td>
<td>each</td>
<td>each</td>
<td>each</td>
<td>each</td>
<td>each</td>
</tr>
<tr>
<td>Filter Size</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Information available</td>
</tr>
<tr>
<td>Protocol</td>
<td>IBM Token Ring</td>
<td>TP/IP, DECNet</td>
<td>TCP/IP, XNS,</td>
<td>TCP/IP, XNS,</td>
<td>Information available</td>
</tr>
<tr>
<td>Suites</td>
<td>XNS</td>
<td></td>
<td>DECNet,</td>
<td>DECNet,</td>
<td></td>
</tr>
<tr>
<td>Analyzed</td>
<td>XNS-MS-Net,</td>
<td></td>
<td>MS-Net,</td>
<td>XNS-MS-Net,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP/IP, NFS, ISO</td>
<td></td>
<td>NFS, VINES,</td>
<td>TCP/IP, NFS,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3+, AppleTalk,</td>
<td>DECNet,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X/VWindows,</td>
<td>XNS-MS-Net,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NETBIOS,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Price</td>
<td>$24,000</td>
<td>$17,350</td>
<td>$15,000</td>
<td>$11,900</td>
<td>Information not available</td>
</tr>
<tr>
<td></td>
<td>(Model 502)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Evolution Of LAN Management Tools
LAN managers, users, software and hardware vendors have all felt the need for a powerful tool to help them deal with LAN-related problems. Along with the growing popularity and complexity of LAN applications, there has been an emergence of tools to manage and troubleshoot problems that are specific to LAN technology.

Existing test and measurement equipment performs services like trapping a user specified network event eg, a line break, collision, or protocol mistake. Time-domain reflectometers (TDRs) can accurately detect line fault conditions. Other available products permit testing of LAN hardware components, eg., ensuring that transceiver cables conform to IEEE specifications, checking transmits, receive and collision characteristics of the transceiver, carrier-to-noise, hum modulation and so on.

All these test equipment offers limited or no insight into the packet data that traverse the network. Over the last few years a new set of sophisticated high performance network diagnostic tools have been emerging on the LAN horizon—the LAN Protocol Analyzers. Protocol analyzers allow the user to examine every byte in the packet data stream traversing the network.

Who Needs A Protocol Analyzer And Why?
Protocol analyzers can be extensively used for developing, debugging, testing and analyzing LAN products. People who develop software or hardware for use on LANs frequently need to see what is going on inside the network. They can use the analyzer to debug software and evaluate the performance of LAN protocols.

System integrators can use analyzers to uncover protocol problems arising due to multi-vendor sources. As the analyzer monitors network traffic, it can perform statistical analysis on various network characteristics. Using the analyzer the LAN manager can simulate various traffic patterns and anticipate load characteristics on the network. Field service representatives will find some of the most profitable uses for this type of product. A person called on to diagnose failures or slowdowns of LANS at client sites can use an analyzer to determine the problem quickly. Even hard-to-
pin-down sporadic problems are easily traced with a LAN analyzer setup for long term monitoring.

Analyzers typically detect virtual circuit error conditions like erroneous CRC, frame misalignment, data runs, jabber when the packet size is longer than specified, preamble errors, illegal network addresses, inter-frame gap errors and so on.

On a single LAN with more than 30 nodes or in an environment with LANS, bridges, and gateways, a LAN analyzer can make it much easier for a busy network manager to keep things running smoothly and efficiently.

Inside a LAN Analyzer

Most of these high-performance LAN analyzers have a personal computer platform with a plug-in adapter card to interface and monitor the particular network type. There is a similarity in the front-end hardware architecture of most analyzers.

Typically, the front-end of an analyzer (Fig 1) consists of a LAN chipset comprising of a network controller and a serial transceiver chip to interface with network. All the frames that are trapped by the card are stored in a RAM area known as the capture buffer. The size of the Capture Buffer varies from 256 K-Bytes to 2 K-Bytes. Besides there is a 16-bit microprocessor on board to communicate with the PC over the X/TAT bus.

LAN analyzers use the Capture Buffer to temporarily store real-time network data. When the buffer’s capacity is reached, the stored data is overwritten by the new incoming data unless the contents are moved to the PC RAM disk. Trace buffer is the area in the PC where the on-line data is continuously transferred for the purpose of displaying information to the user. Various trace buffer implementations include RAM disks, expanded memory and direct logging to hard disk.

It is imperative that the analyzer does not miss a single frame at high data rates. To cope up with high data rates (10 M-bit/sec for Ethernet and 16 M-bit/sec for Token Ring), special data filtering and slicing techniques are used to make best use of the capture and trace buffer.

Capture filters are a set of user-defined hexadecimal byte pattern templates that let the user selectively store packets in the capture buffer. If there is a match between the template and the incoming frame, the frame is stored in the buffer, otherwise it is discarded. The filter size varies from 2 bytes to 2 K-bytes and the filtering mechanism is implemented in hardware or software. The former implementation is faster, more efficient but complex.

To do event-driven analysis, filters can also be combined to define capture triggers that allow the user to capture a specified number of packets before and after a given event occurs. This can be very useful while setting up the analyzer for long duration to debug transient problems. Some analyzers can also be setup to respond to external triggers, or to generate an output on the serial port when data causes a trigger. The other technique that is used for efficient buffer usage is known as slicing. At protocol headers in any frame are contained in the first 128 bytes or less, users in most applications have no need to view the data portion in the frame. Analyzers allow the user to specify a slice size which allows retention of the frame up to the slice size only and the rest is discarded. Since all analyzers are restricted by a finite size of capture and trace buffers, slicing combined with filtering allows capture of a large number of relevant network data and thereby efficiently using the buffer space.

Captured information is immediately available for display and analysis. Some analyzers allow filters during display known as display known as display filters on top of real-time filtered data for better accuracy.

Protocol decoding, translation and interpretation at all layers of the OSI model occur during the display analysis phase. It provides the user with organized information about the protocol content of the selected frames in addition to address, timing, frame size, cumulative byte count, and frame sequence number.

A wide variety of display formats are provided to ease interpretation of the captured frames. These choices range from summary views, depicting 15 to 20 frames at a glance, to detailed views of individual frames with information...
Introducing Reliable dBASE IV.

dBASE IV Version 1.1 is brought to you in India by Wirpo Systems Ltd., a leading software house and exclusive distributor of Ashton-Tate products in India. Along with every package of dBASE, the user is entitled to free training, a 90-day warranty and unlimited telephonic support. Registered users of dBASE IV Version 1.0 get dBASE IV Version 1.1 free.

Your wait is over. Call us or write to us.

Wirpo Systems Limited
40 A Lalit Road
Bangalore 560 001

WIRPO SYSTEMS

Capabilities Of A LAN Analyzer

A LAN analyzer is a very powerful diagnostic, troubleshooting and analysis tool. Its versatile and wide range of capabilities allow a LAN manager to troubleshoot a network hardware or software problem, to monitor network performance or to debug a network application. We shall look at some of the salient features of an analyzer and discuss, in general, how the analyzer can be used to manage a LAN.

- **Observe General Network State**
  - Most analyzers allow the user to collect and observe general statistics about the activity on the network. To do this, the user sets up a network monitoring session on the analyzer and selects the kind of statistics he/she is interested in.
  - The user can also select the visual form e.g., tabular, pie chart, bar graph etc. for display of information and can record the session in a file for later viewing.

Typically the following sets of statistics can be viewed:

a) Network utilization & throughput
   - Network utilization measures how much a network is being used as a percentage of the maximum network speed ("network bandwidth"). For example, Ethernet can operate at the maximum of 10 M-bits/sec, whereas the actual network throughput may be much less depending on various factors like collision, frame size etc.
   - This group of statistics also includes behavior of network utilization in frames per second, percentage of good and bad frames etc.
   - This statistics is most useful in finding out whether a network is performing well and is usually the first step in diagnosing most problems.

b) Error distribution of frames
   - This statistics shows the number and percentage of frames having one or more errors.
   - This is useful in checking whether there are abnormally large number of error frames and if a particular type of error dominates the error pattern.

c) Length distribution of frames
   - This shows the number and percentage of frames falling into various length ranges along with average, peak and minimum frame lengths. This statistics is useful in verifying, for instance, if too many short frames are loading the network.

d) Interframe spacing distribution
   - This gives number and percentage of frames falling into one of a set of interframe gap ranges. This is useful in identifying network jamming by short back-to-back frames.

- **Observe Node Behaviour**
  - These statistics are useful in observing behavior of a set of particular nodes in the network which include:

a) Node statistics
   - This statistics focuses on a particular node and gives complete details of its behavior during a session e.g., number of frames and bytes trans-
mitted, length distribution of frames, distribution of error frames generated by the node, timings of frames transmitted etc.
b) Connection statistics: This statistic depicts complete results of monitoring a connection ('session') between two particular nodes. This can be used to identify causes of communication problems between particular nodes.
c) Communication statistics: This group of statistics presents source versus destination tables, summary of nodes contacted by the particular node, connection duration distribution etc.
- **Capture Frames**
  This is one of the most important features of a LAN analyzer which allows the user to examine the contents of the captured data. The user has various options by which he/she can specify real-time filters, trigger conditions etc. At capture time, the user typically can see only certain minimal information about the network. After the capture session is over, he/she can explicitly examine the captured data in detail.
- **Examine Frames**
  This is the most powerful feature of a LAN analyzer which allows the user to examine the minutest details of each frame. Automatic protocol decoding is done for the protocol header of each frame and the information is presented to the user in the most detailed form aided by color coding or grey scale shadings to demarcate protocol layers. Detailed decoding is carried out on bit or byte level fields within each protocol. This mode is extremely useful in debugging specific problems related to protocols and wherever the user needs an insight into the protocol layers in a frame. With the proliferation of various protocol suites e.g. DNS, Decnet, RDP, etc., a LAN analyzer is characterized by the number of such suites which it can decode. Often, the user has the option of buying protocol decoding suites at incremental costs depending on what protocols are being used in the user's network.
- **Maintain Network Database**
  Some analyzers allow building of complete databases about all the nodes in the network having information like node name, address, machine name, network card vendor etc. The user can also keep details of segmentation and multiple networks in the database. The user is also supplied with functions to add, modify, delete entries in the database. Often during frame decoding, instead of node addresses the user is presented with the symbolic name of the node as entered in the database thereby easing understanding.
- **Simulate Network Traffic**
  In this mode the passive analyzer becomes an active frame source. The user can control the frequency of transmission and put known data in the frames. Frames with error can also be simulated. Sending known traffic is useful in debugging faulty node behavior, predicting network utilization under different load conditions etc.
- **Perform Cable Test**
  Most analyzers have built in TDRs to diagnose and pin point faults in LAN cables or connectors and generate detailed report about the location and type of the fault like cable open or short.

**Survey of Network LAN Analyzers Available in The Market**

The survey (as shown in the table on page 61) of some higher-end LAN analyzers from various manufacturers lists the hardware and software characteristics coupled with their prices.

**Selecting For Your Needs**

LAN standardization has changed the way computer systems are designed, developed and maintained. It has caused users to shift from using a sole source vendor to seeking a multi-vendor heterogeneous system/networking solution.

Network analyzers provide the type of in-depth information necessary to keep a networking system operating at peak efficiency. Selecting the best analyzer, however, is not easy. There are many price ranges and options from which to choose. Indeed, the base retail list prices for analyzers under discussion range from $10,000 for module-level products (add your own PC) to $20,000 or more for complete hardware/software configurations. Selecting the proper analyzer for your needs requires a detailed look at the market and your individual requirements.