Law of the LAN

Diane W. Savage
Just when we were getting comfortable with the lingo of the PC era — filled with bits, bytes, RAM, ROM, MS-DOS, and PC-DOS — computing has moved into a new age. Local area networks, or LANs, define this new era in which the LAN is the computer, and the vocabulary is a virtual alphabet soup of acronyms such as LAN, WAN, CMIP, SNMP, OSI, TCP/IP, and SNA among others. The growing use of LANs is having a dramatic effect on the manner in which computer software is licensed. Although a basic understanding of LANs is necessary in order to draft an appropriate network software license, it has proved difficult for lawyers to develop an understanding of this complicated and evolving technology. Glossaries of LAN terms are widely available; however, there is a dearth of lay-oriented literature tying these many terms together.

The purpose of this article is to use these terms interactively to define what constitutes a LAN, outline the history of the LAN, describe the hardware “regions” which comprise the LAN, and its software “governance.” Since it has become necessary for LANs to communicate with other LANs, this article will also describe the rudiments of the “international law” of interconnectivity. This article will also address three legal issues which become critical in the context of network licensing because of their economic impact. First, the time honored method of licensing software per CPU is inadequate for networked environments and the growth of networks has given rise to a variety of alternative methods of licensing software for use on LANs. Second, increased reliance on LANs to run mission critical applications, coupled with the rapid growth in computer viruses, has created a new software warranty, known as the computer virus warranty, which is increasingly required by sophisticated software customers. Finally, writing a software program for use on a LAN is more complicated than writing the single user version of the same software, and its proliferation over a LAN dramatically increases the potential economic consequences of an
error, or "bug," in the software. Just as software developers are learning how to develop, install and maintain "network aware" software programs, their lawyers need to learn how to draft "network aware" licenses which responsibly address these issues. The attached appendix will provide examples of "network aware" contract provisions which address these legal issues.

WHAT IS A LAN?

A LAN is a data communications facility that interconnects a number of data transmitting devices, like computers and terminals (these transmitting devices are frequently referred to as "nodes"), and allows for the exchange of data. A LAN is confined to a relatively small area, such as a building or a group of buildings, in contrast to a wide area network (WAN) which may span a large area such as a continent, or a metropolitan area network (MAN) which may span a small city or a town.

The three key elements of a LAN are its: (1) topology, (2) transmission medium, and (3) access technique.

"Topology" refers to the LAN's physical layout, or the way in which the nodes in a network are connected together. There are three major LAN topologies. These are:

- the bus topology;
- the ring topology; and
- the star topology.

There are also a number of hybrid network topologies which combine features of the above topologies.

In a bus topology, the communications network is a single length of the transmission medium onto which the various nodes are directly connected. This topology is used in traditional data communications networks where the host at one end of the bus communicates with several terminals along its length.

---

1. The global telephone network is the largest communications network in the world. It serves the needs of voice users well, but is an expensive and inflexible system for data communications. As the proportion of interoffice communication accounted for by data increases vis-a-vis voice, the need for an integrated voice and data service also increases. The change to an integrated service is also outside of the scope of this article, but it involves two approaches. First, the traditional telephone network is evolving into a network known as the Integrated Services Digital Network (ISDN). This standard specifies the interface through which a user may transmit voice and data using telephone switches. Second, integrated services may be offered by an Integrated Service Local Network (ISLN), in which the underlying network is a LAN with interfaces which can carry voice traffic.

2. This article will not address WANs or MANs, which are also outside its scope.
In a ring topology, the nodes are connected on a single transmission medium which forms a closed loop. Each node on the LAN acts as a repeater, and data travels through each node. The IBM Token Ring is a star ring or a star-shaped ring and is the most common example of this topology. Because of IBM's Token Ring Network, this topology is expected to gain at least 70% of the local area network market in the next few years.3

RING

Star topology uses individual data paths from a central hub or concentration point to each node. All data must pass through the hub, just as all telephone calls pass through a central switching station. The pure star topology is not used frequently in data communications, but it is used in IBM 370 installations and in office PBXs.4

---

4. BRENDAN TANGNEY, DONALD O’MAHONY, LOCAL AREA NETWORKS AND THEIR APPLICATIONS, 16 (1988).
LANs must also have a connecting medium of some sort to carry the information from node to node. Many different types of media may be used. The most common forms of transmission media are twisted pair, coaxial cable and optical fibers, although microwave transmission, infrared transmission, and telephone lines may also be used.

Bus and ring topologies require that the transmission medium is shared between a number of nodes. This means that there must be a mechanism for transferring chunks of data from one node to another and another mechanism which ensures that one node's transmission does not interfere with any other node's transmissions. The first mechanism is packet sharing and the second is access control. In packet sharing, data is collected in packets which are launched into the network. The common elements that make up a typical packet are: (1) the start of packet indicator which informs other nodes that a packet is being transmitted; (2) the address of the sender and the receiver; (3) the control field which states the pur-

5. *Id.* at 9.
pose of the packet; (4) the data field which contains the data to be transferred; and (5) the error check field, which allows the network hardware to detect transmission errors.\(^6\)

In access control, the many nodes on a LAN which may wish to transmit data simultaneously are regulated by following a common access method; all nodes observe the same procedures in order to send data. Access control methods can be divided into contention and non-contention methods. In a contention-based access method, a node seizes the opportunity to transmit when the network becomes idle. The most common contention method is Carrier-Sense Multiple Access with Collision Detection (CSMA/CD). With CSMA, the physical layer of a user's workstation generates a carrier-sense signal and listens to detect any other carrier-sense signals from other nodes. If no other signal is detected, the user sends his or her message. However, if two nodes are located far apart, the first node may not detect signals from the second node, with the result that the two nodes commence transmission simultaneously and a data collision occurs. Collision Detection (CD) means that the two nodes listen while they transmit a message. If they detect a data collision, each node waits a different random amount of time before sending the message again.\(^7\)

In a non-contention based access system, a node that wants to transmit data must wait to receive "permission." With one popular non-contention based system called token passing, a free token is passed from one node to another. When a node has taken possession of the token, it has permission to transmit a data packet, and then it passes the token to the next node in the sequence. As Stan Schatt explains in his book *Understanding Local Area Networks*:

To understand how this token approach contrasts sharply with the CSMA/CD bus approach, imagine a public forum on a controversial issue. Under the CSMA/CD method, several people might try to speak simultaneously only to stop speaking when they hear another speaker begin. With dozens of speakers trying to speak yet not wanting to interrupt each other, the process would become chaotic and inefficient. With the token approach, a token would be accepted as a symbol of authority giving a person a right to speak. Whoever held the token would stand and make a speech. When finished, he would pass this symbol of authority to the next person who desired to speak. No one would attempt to speak without physically possessing the token.\(^8\)

\(^6\) *Id.* at 27-29.
\(^7\) *Schatt*, supra note 3, at 41.
\(^8\) *Id.* at 41-42.
LAN History

The first computers in the 1940's and 1950's were mainframes which occupied entire buildings. Because they were so expensive, they were available to only a limited number of users. In the 1960's, groups within organizations began to share these high-priced mainframe computers through the use of a primitive network consisting of "dumb" terminals connected with a mainframe computer through telephone lines. Through time-sharing, these various groups within an organization could enjoy the benefits of the mainframe computer without massive capital expenditures, although this time-sharing arrangement could be quite slow.

During the 1970's, minicomputers became available at dramatically reduced prices which enabled work groups to purchase their own computers. This concept of distributing computers throughout an organization by providing groups with their own minicomputers was known as "distributed processing." However, these distributed minicomputers needed to communicate with each other, thus organizations began cabling them together and writing software to enable such communications.

These first experimental local area networks appeared in the 1970's. In 1974, IBM announced its System Network Architecture (SNA) and in 1975 Digital Equipment announced its Digital Network Architecture (DNA). The establishment by major computer manufacturers of their own proprietary network architectures led to a situation where a major manufacturer's computers could communicate easily with each other, but communication among multiple manufacturers' computers was difficult or infeasible. This meant that smaller companies were at the whim of larger manufacturers, who could change their architecture at any time, leading to a demand within the industry for a standard communications architecture.9

In 1978, the International Standards Organization (ISO), based in Geneva, Switzerland, released a reference model for computer networking known as the Open Systems Interconnection (OSI) Model.10 The OSI Model represents a standard approach to communicate information throughout a network, so that a variety

---

9. TANGNEY & O'MAHONY, supra note 4, at 87-88.
10. The OSI, SNA and TCP/IP architectures are the most popular LAN architectures today and can be used on top of any LAN. The Transmission Control Protocol (TCP) and Internal Protocol (IP) issued by the U.S. Department of Defense is currently the most widely available architecture. Like the OSI model, the TCP/IP architecture is layered, but it contains only the following four layers:
of independently developed computer devices can operate on the network. In 1984, ISO released a revised version of the OSI Model which has become an international standard. The OSI Model separates the communications and computing functions provided by LANs into the following seven layers:

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>Application</th>
<th>Presentation</th>
<th>Session</th>
<th>Transport</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Higher Layer Protocols</td>
<td>Ethernet, Token Ring</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Physical and Data Link layers of the OSI Model establish rules for cabling media, transmission speed, physical topology, and access method of the LAN. The five higher layers provide the methods by which information is reliably transmitted between sending and receiving nodes on LANs and other attached networks, and the way such information is processed and presented to the user. Each layer performs its functions by invoking the services provided by the layers below it, then it returns the results to the invoking layer above. This layering of protocols is a basic principle of standards-based networking. 11

<table>
<thead>
<tr>
<th>Layer</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Application</td>
</tr>
<tr>
<td>3</td>
<td>Transport</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>1</td>
<td>Network Access</td>
</tr>
</tbody>
</table>


11. In Understanding Local Area Networks, Stan Schatt uses a citizens band radio to illustrate the principle behind the OSI layers. The CB user first presses his send button and announces, “Breaker, breaker” to indicate that he wants to send a message. He then identifies himself with his nickname before asking his friend for her nickname: “This is Happy Hacker, can you read me PC Woman?” After making contact, he asks his friend to switch over to another channel because it is clearer, and his friend acknowledges by replying, “That’s 10-4, Happy Hacker.” At the physical layer, Happy Hacker pressed certain buttons to broadcast his message. His use of nicknames constituted the second communication layer, established a concrete address for the recipient, and identified himself as the sender. The third layer of communication occurred when he determined the quality of the transmission
In 1980, the Institute of Electrical and Electronic Engineers (IEEE), a U.S. standards making organization, formed a committee known as Project 802, whose task was to work within the scope of the OSI Model to develop a set of standards for local area network topologies and medium access control methods. Project 802 divided the Data Link layer of the OSI Model into two sublayers: a Logical Link Control sublayer (LLC) and a Media Access Control sublayer (MAC). The LLC is concerned with providing a data link service to the higher layers, while the MAC concentrates on providing shared access to the Physical Layer.

Project 802 also produced three IEEE 802 standards of particular interest. The IEEE 802.3 subcommittee established an Ethernet standard for LANs. It also established the CSMA/CD protocol referred to earlier, which specifies the way that a LAN using bus technology should construct its data packets and send them over the network to avoid collisions. The IEEE 802.4 subcommittee developed Token Bus, a token passing collision prevention standard for a different type of bus network which is frequently used in factory automation. The IEEE 802.5 subcommittee established another standard, Token Ring, to cover networks with ring topologies that use a token to pass information from one workstation to another. Token Ring is the principal PC LAN technology supported by IBM. Ethernet and Token Ring have become the dominant Physical and Data Link layers for LANs.

The growth of the use of PCs and workstations in the 1980's resulted in the need for users to communicate with each other through their common databases and software and to share peripherals. By the late 1980's, the need for LANs was universally accepted. Today, networking is the fastest growing segment of the computer market, according to Doug Gold, an analyst with Inter-
national Data Corp. in Framingham, Mass.14 The shipment value of complex LAN and internetworking products, software, and related services totalled $4.7 billion in 1989 and is expected to increase to $11 billion per year by 1993.15 With this rapid growth of LANs, experts estimate that the percentage of terminals, personal computers, and workstations which are interconnected by LANs will grow from 15% in 1989 to 83% in 1993.16

COMPONENTS OF THE LAN

LAN Hardware

A LAN is built from the following hardware devices: (1) servers; (2) workstations; (3) transmission media; (4) network interface units (NIUs); and (5) a hub, concentrator, or wiring center. Just as each state has a governor, each workstation has its own operating system software to control local activities. Each country has a chief executive officer, and each LAN has a network operating system, which typically resides in the central file server (the "national capital" of the LAN), to control the activities of the LAN.

Most LANs start out as a homogeneous set of equipment from a single vendor which share a common set of rules, which are frequently referred to as "protocols." As the network grows, however, hardware and software from different vendors using different protocols are added, and the management of the LAN grows more complex. The Network Management System discussed in this article mediates between the protocols of various hardware on the LAN by focusing on standards.

Servers. The network operating system, shared data, and shared applications reside in the server, which is the electronic equivalent of an office filing cabinet. There are two types of servers:

- In client/server LANs, a dedicated "file server" provides a common service to all other workstations, also referred to as "clients," on the LAN. For example, one or more computers might be dedicated to storing files of information for all other computers on the LAN, which can ask these file servers to deliver copies of files on command. Another set of computers might be dedicated to providing laser printing services ("print servers") or access to catalogued information in on-line

databases ("database servers"). A dedicated server is not available for running programs.  

- In server-less, or peer-to-peer LANs, each workstation can also be both a client and a "mini-file server" for all other clients on the LAN. Each user can decide which disks or files to make available or publish. Other clients can then access that information across the distributed network. Some believe distributed systems enhance reliability because they theoretically allow multiple repositories for shared data rather than a single main file server as in a client/server LAN.  

Workstations. Workstations may include IBM computers or compatibles, Apple Macintosh computers, Unix-based and other engineering workstations, and diskless workstations. The workstation is provided with data from the file server, and the actual execution of the application programs occurs at the workstation.

Transmission Media. Transmission media connect the nodes on the LAN. There are three commonly used forms of transmission media:

1. Twisted pair cabling, the most common form of wiring in data communications consisting of two insulated copper wires arranged in a regular spiral pattern, is the least expensive type of network cabling. Twisted pair comes in unshielded (ordinary telephone wire) and shielded (shielding with metallic braid that reduces interference). Shielded twisted pair provides better performance at lower data rates than unshielded twisted pair, but it is more expensive and more difficult to work with.

2. Coaxial cable, composed of a single inner wire conductor surrounded by insulation with an outer jacket of aluminum or copper, is more expensive than twisted pair, but supports both broadband and baseband LANs. Baseband coaxial cable has one channel that carries a single message at a very high speed. Broadband coaxial cable can carry several different signals broadcast at several different frequencies at the same time, and therefore can accommodate integrated voice, data, and video signals. This type of cable is frequently found in homes as a part of cable television.

---

19. An alternative to transmitting the information over cables is to transmit it using infrared or microwave radiation. Although it is impractical in the usual office situation, it can be useful for communicating between buildings. TANGNEY & O’MAHONY, *supra* note 4, at 12-13.
(3) Optical fiber, consisting of a pure glass cable drawn into a very thin fiber to form a core, is the most expensive type of network cabling, based on media and installation cost. Optical fiber uses analog signaling to carry data in the form of modulated light beams. Optical fiber is used for very high speed and/or high capacity data communications needs. One type of network that uses fiber optics is Fiber Distributed Data Interface (FDDI). 22

Network Interface Units. Network Interface Units (NIUs) are the cards that plug into a workstation or server to connect it to the transmission medium. The NIU contains logic for accessing the LAN and for sending and receiving data packets on the LAN. 23 The main task of the NIU is to form these data packets from the workstation and transmit them onto the transmission medium. The NIU also receives data packets from the transmission medium and translates them into bytes which the workstations can understand.

The Hub, Concentrator or Wiring Center. Each workstation on a network needs access to the file server. However, it is usually not possible to have every workstation directly attached to the file server. To accommodate multiple workstations, a hub or central wiring center may be used, although certain network architectures (like ring topology) do not require hubs. 24

LAN Software

The Workstation Operating System. The operating system for each workstation is loaded at the workstation and acts as the “governor” for the workstation, controlling the execution of other software on the workstation. The workstation operating system also includes, or works in conjunction with, software created by the network operating system which is loaded on the workstation. Each network operating system has a different name for this piece of software, which is sometimes referred to as a “requestor” or “redirector,” and which determines whether the requests made by the workstation are for local processing or network processing. If the request is one for local processing, like copying of local files or formatting of local media, it is serviced by the workstation operating system. If the request is one for network processing, it is serviced by the network operating system. The workstation operating system is essential for the workstation to operate, even if it is not a part of a network. The workstation operating system conceptually

22. STALLINGS, supra note 10, at 48.
23. Id. at 6.
resides in the Presentation Layer of the OSI Model.25

The most popular workstation operating system today is MS-DOS from Microsoft, which is found on IBM PCs and compatibles. Because DOS was originally designed as a single user operating system, most PC LAN implementations have been forced to take a three-tiered approach to network governance consisting of DOS, NIUs and a separate network operating system. However, IBM's newer OS/2 operating system is an integrated operating system which includes both workstation and network operating system components. As a result, OS/2 eliminates the need for a separate network operating system.

The Network Operating System. The network operating system controls all network activity. The network operating system manages access to the data on the hard disks of the file server, handles security of the data on the file server's storage devices, communicates between the user and the network, accesses network services, accesses shared printers and other servers, and accesses shared outside services such as gateways and bridges. The most common network operating system on the market today is NetWare from Novell.26 NetWare offers a fairly complete suite of network protocols, and there are more products available for NetWare than any other LAN operating system.27 The network operating system conceptually operates at the Application Layer of the OSI Model.

Network Applications Software. The challenge for the 1990's is for software companies to develop a new type of LAN applications software. The packaged software of the 1980's, primarily designed for use on standalone computers, is inadequate because it cannot anticipate all of the combinations of hardware and software on which an application must operate in a network and because it is not designed to take full advantage of the communications features of the network. According to Patricia Seybold, president of Office Computing Group, a Boston consulting firm, new network application software is "where all the action is, and where it's going to be for the next 10 years."28

The development of network applications software requires a

25. Id. at 23-24.
radical change in the software which software suppliers develop, as well as the way they market, distribute and support software. Although most standalone software today is “networkable” (which means that it is able to function on a network without additional changes), there is an increasing demand for “network aware” software — software which is designed from the ground up to run efficiently in a networked environment. Both networkable and network aware software generally include file locking functions, and may include a license manager utility to restrict software usage. However, network aware versions generally include additional features which make them more adept at handling the hardware and software configurations of multiple users, such as record-locking, customized start-up files which let users call the application from a server using appropriate device drivers for their particular workstation configuration, file transfer facilities, and facilities to access other remote peripherals. Network aware software frequently takes the form of groupware, which includes office automation type functions like group calendaring, project management, voice messaging, e-mail, and call tracking.

Writing network aware software is an order of magnitude more complicated than creating the single user version of the same program. An example of a problem conversion of a single user software system to a network specific version was Ashton-Tate’s Multiuser dBASE II, which Ashton-Tate withdrew from the market. According to Ashton-Tate’s public relations manager, “it could have corrupted some data,” although “it was not a major bug” that stopped shipment of the network specific version. More recently, DSC Communications Corporation reported that three binary digits set incorrectly in minor software updates to its call-routing switches knocked out telephone service to ten million people in

29. A “file lock” provides the ability to lock a file so that only one user may use it at a time.
30. A “record lock” provides the ability to lock a record so that several users can share the same file at one time, but cannot share the same record within a file.
32. “People who have been around the computer track a few times think all LAN products should carry a label: WARNING! Use of this product could be hazardous and possibly fatal to your business health! Like alcohol, chocolate and television, networks carry a large potential for abuse. Your level of involvement must be balanced against the wisdom of keeping a safe distance away from any volatile, unstable substance. Think of LANs as nitroglycerine: this would give you just the right amount of respect for their exposure potential.” John Hawkins, Networks: the creatures with two heads; the perils of being a network consultant, DATA BASED ADVISOR, November 1989, at 12.
33. Keith Yocum, Software Shortage Has LAN Industry Tied Up, PC WEEK, April 2, 1985, at 52.
five states and the District of Columbia. Congressmen and witnesses testifying at a hearing on the outages stressed that telephone companies should have better contingency plans for dealing with disruptions "that are certain to occur as network software becomes more complex."\(^{34}\)

Network aware software also involves substantially more support from the vendor to customize the software for the users' needs and to install the software on the network. As a result, Patricia Seybold estimates that for each dollar which a company spends on software for networks, it spends five dollars on consulting systems, integration and custom programming.\(^ {35} \) An example of this is Lotus Notes, a groupware program that runs on PCs and enables workers on a network to communicate more effectively. Notes customers who pay $62,500 receive a programming system, 200 copies of Notes, five days of consulting and six months of technical support.\(^ {36} \)

This move to consulting is something of a "back to the future" strategy. Thirty years ago, computer companies sent teams of programmers to their customer's sites to develop custom software for their new mainframe computers. This changed in the 1980s, when independent software companies emerged to supply prepackaged software for use on PCs. In the new networking era, software companies are discovering that demand for consulting and custom software development is growing rapidly as corporate customers begin to move large applications from mainframes to PC-based LANs. For example in 1991, one year after Microsoft launched its consulting unit, it had 200 consultants in seven countries working for over 150 clients to meet their needs for consulting and custom software development.\(^ {37} \)

**The Network Management System**

The Network Management System consists of hardware and software additions which are implemented among the network components described above. The Network Management System views the LAN as a unified architecture, with addresses and labels assigned to each node, and the specific attributes of each node known

---

36. *Id.* at 104.
to the system. ISO has suggested the following five key areas of network management:

(1) **Fault Management.** When fault occurs, the Network Management System should be able to determine the location of the fault, isolate the rest of the network from the failure, modify the network to minimize the impact of operation without the failed components and repair or replace a failed component to restore the network to its initial state.

(2) **Accounting Management:** The Network Management System should be able to track the use of network resources by user and user class for planning network growth, as well as for internal accounting purposes, to determine whether a user or group is abusing access privileges or whether users are making inefficient use of the network.

(3) **Configuration and Name Management.** The Network Management System should control initializing a network and shutting down part or all of the network, as well as maintaining, adding and updating the relationship among its components and the status of components during network operation.

(4) **Performance Management.** The Network Management System should be capable of tracking activities on the network and enabling performance management to make adjustments to improve network performance (e.g., by controlling capacity use level, excessive traffic and response time).

(5) **Security Management.** The Network Management System should monitor and control access to the network and to all or part of the network management information from network nodes.\(^{38}\)

The Network Management System is typically comprised of one or more Network Control Hosts and associated software commonly known as the Network Control Center and the Network Management Entities.

**Network Management Hardware.** In today's world, each vendor's equipment may be managed by a different workstation (commonly called an "element manager"). However, in an Integrated Network Management System (INMS) that manages many types of LAN to WAN connections and devices, one or more workstations are designated as the Network Control Host.

**Network Control Center.** The Network Control Center is a collection of software which resides on the Network Control Host.

---

38. STALLINGS, supra note 10, at 251-255.
The Network Control Center includes an operator interface so that the designated administrator can manage the network. The Network Control Center responds to user requests concerning the LAN by displaying information and issuing requests for information to Network Management Entities, described below. This communication is carried out with an Application Layer network management protocol that uses the communications architecture in the same fashion as any other distributed application.39

**Network Management Entities.** Each network node contains a collection of software known as the Network Management Entity, which is dedicated to certain network management tasks. The Network Management Entity collects and stores statistics on network related activities, and responds to requests and commands from the Network Control Center.

Because network management software relies on the host operating system and communications architecture, most Network Management Systems today are designed for use on a single vendor's equipment. However, vendors of Network Management Systems are focusing on two protocols that are emerging as open network management standards to permit these systems to manage multivendor networks — TCP/IP based simple network management protocol (SNMP), which is maintained by the Internet Activities Board, and common management information protocol (CMIP), which is based on standards set by ISO. These protocols provide a common format for network devices such as bridges, routers, concentrators and modems to communicate management data via an "agent" to the Network Control Host. In addition, CMIP allows communications among different Network Management Systems. The move toward multivendor support will provide administrators of large heterogeneous networks with critical long term advantages. For example, network administrators will be able to monitor and control multivendor networks from a single point in the network.

All Network Management Systems handle multiple protocols in the same way. SNMP management information bases (MIBs), CMIP objects and attributes, and the proprietary definitions of managed objects in the network are grouped together in the Network Management System's memory according to the types of devices that the system handles. Translation routines, which match the object definitions with what they manage in the network, are

---

39. *Id.* at 259-262.
handled in one of three ways. The first approach is to handle this translation on the Network Management System, whether it is an Integrated Network Management System (INMS) that manages many types of LAN to WAN connections and devices, or an element manager that handles just one kind of device. The second approach, used by IBM and AT&T, is to use an application program interface (API) to handle conversions between standard and proprietary protocols. The API is provided to third party vendors, including other network management vendors and companies that manufacture element management stations, which can then map their proprietary routines to the API. The third approach is to put the burden of protocol translation on the applications that run on the managed devices in the network. Using this approach, each managed device contains a software protocol gateway that converts incoming messages from the Network Control Center to its own protocol.

INTERCONNECTIVITY: THE INTERNATIONAL LAW OF LANS

As LANs become more prevalent, the need for LANs to communicate with each other becomes more pronounced. The underlying objective of interoperable products is to facilitate a union of a number of LANs through the establishment of protocols which govern the exchange of information among participating LANs. To carry out this objective, four major components are used: repeaters, bridges, routers, and gateways (or backbones). These products perform tasks to achieve compatibility among LANs at different levels of the OSI Model as follows:

41. *Id.* at 51.
42. Richard Pastore used a similar metaphor to point out the need for such protocols: "An archipelago of isolated islands, each with its own native language and customs. It sounds idyllic — unless you're talking about islands of data distributed across several local-area networks. Then the image becomes a Bermuda triangle of lost data integrity, data inconsistency and incompatible security protocols." Richard Pastore, *LAN Ho! Navigating Downsized Data*, COMPUTERWORLD, June 4, 1990, at 67.
<table>
<thead>
<tr>
<th>Device</th>
<th>OSI Model Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway/Backbone</td>
<td>Level 7 Application Services</td>
</tr>
<tr>
<td>Gateway/Backbone</td>
<td>Level 6 Presentation</td>
</tr>
<tr>
<td>Gateway/Backbone</td>
<td>Level 5 Session Control</td>
</tr>
<tr>
<td>Gateway/Backbone</td>
<td>Level 4 Transport</td>
</tr>
<tr>
<td>Router</td>
<td>Level 3 Network</td>
</tr>
<tr>
<td>Bridge</td>
<td>Level 2 Data Link</td>
</tr>
<tr>
<td>Repeater</td>
<td>Level 1 Physical</td>
</tr>
</tbody>
</table>

**Repeaters.** Although repeaters are categorized as internetworking devices, they actually connect segments of the same network to form an extended network. In other words, repeaters are used when a LAN wants to expand its own boundaries rather than to govern the relationships between two LANs. A repeater is not used to interconnect different networks: it is used to "repeat" the electrical signal between cable segments and physically extend a single network. The repeater functions at the lowest level of the OSI Model, the Physical Layer, and its sole function is to extend the maximum length that a signal can travel, thereby extending the physical size of the network.

**Bridges.** Bridges connect two similar LANs that use identical protocols. Bridges are divided into those that connect LANs in the same site (local bridges) and those that make use of telecommunications facilities to interconnect LANs at different sites (remote bridges). The bridge picks up data packets from one LAN that are intended for a destination on another LAN and passes these packets on. Each time the bridge transfers packets between networks, it also acts as a repeater to regenerate the signals. The bridge does not modify the packet or add anything to it. The bridge is more intelligent than a repeater in that it can look at the header of a data packet and determine to which of the two networks the packet belongs. Bridges operate at level two of the OSI Model, the Data Link Layer, so layers three and above must be identical in the two systems for successful communications in a bridge.

**Routers.** Routers are used to interconnect networks that may or may not be similar. The router operates at level three of the OSI Model, the Network Layer, sometimes known as the internet proto-

---

46. *Id.* at 187-191.
col. This internet protocol is present in each router and in each host on the network. In addition, as with the bridge, each host must have compatible protocols at layers four and above in order to communicate successfully.47

**Gateways and Backbones.** Gateways are the most complex interconnectivity devices. The gateway is used to connect computers that use different communications architectures. The gateway functions on all seven layers of the OSI Model so it can be used to connect OSI-based products with proprietary products, like a LAN using IBM’s SNA architecture. The gateway maps from an application on one computer to an application that is similar in function, but which differs in detail, on another computer.48

Networks with different communication architectures can also be connected via a backbone network. A backbone network is a control network to which other LANs are attached. Fiber optics are usually used for backbone networks because backbones require a larger bandwidth and need to be able to transmit across long distances. The LANs are attached to the backbone network via bridges, routers, or gateways, depending on the architectures of the LANs and of the backbone.49

**“NETWORK AWARE” LICENSE ISSUES**

**Methods of Licensing Software For Use on LANs**

Software companies are changing the way they do business because computer networks are changing the way companies handle information. The use of mainframes in the 1960’s did not provide individual workers with the tools they needed to do their jobs. PCs, on the other hand, provided job-specific tools, but did not let workers share information or work collaboratively with each other. Groupware on LANs is allowing workers to coordinate their activities through e-mail and office automation-type functions like voice messaging, project management, group calendaring and call tracking.

The increasing use of software on LANs has resulted in a demand by users for a consistent, common way to license, distribute and administer applications software across a network. The time-honored licensing practices of licensing shrinkwrapped software either per processor or via a by-site license are inadequate for

47. *Id.* at 207.
48. *Id.* at 210.
49. *Nunemacher*, *supra* note 24, at 142-144.
networked environments where applications are shared by users on heterogeneous computers and where the network itself is constantly changing size and configuration.  

Software companies, on the other hand, are concerned that LANs present a real threat to their economic survival. When a network administrator buys a single-use copy of a software program and lets ten people on the network access that program simultaneously, the software company loses a lot of money. As a result, software companies which were forced by the marketplace to drop copy protection schemes during the mid-1980's are now implementing such schemes again in the context of LAN licensing.

Rather than balking at such schemes, sophisticated computer users are asking for them. The network administrators in a recent Software Publishers Survey unanimously favored lock-out systems. The Survey reported that:

One administrator complained adamantly about publishers that do not provide this utility in network versions of software: "They provide a LAN edition and then basically say 'you control it,' without giving you the tools to do it. It's asking for problems."  

The growth in LANs has resulted in a plethora of license approaches. "We get a lot of calls from network administrators who have some problem where they're running 10 different packages and they are licensed in all sorts of different ways," says Ann Stephens, research director for the Software Publishers Association. "It can make for all sorts of headaches as far as controls go."  

The following example illustrates the problem.

A company with 200 employees, 100 workstations and three file servers, loads an application program on all the three file servers. No more than 80 employees ever use the program, and there are never more than 60 users at one time. However, the amount charged for such use will vary based on the license model which the software supplier has adopted.

- **Per CPU licensing** - the customer pays for 100 licenses.
- **Per User licensing** - the customer pays for 80 licenses.
- **Server-based licensing** - the customer pays for three server licenses.

---

Site licensing - the customer pays a negotiated fee for unlimited use within a defined site.

Concurrent Use licensing - the customer pays for 60 licenses.

1. Per CPU licensing. Some software suppliers license their software for use on a single CPU.53 This license scheme is easier for network administrators to manage than per user licensing. However, it may be uneconomic for users if some workstations require only occasional access to the software program. In addition, users may have files on unlicensed CPUs which require complicated file transfers to use with the software programs on the licensed CPUs.

Some software suppliers enforce their per CPU licensing approach with node-locking. A node-locked license ties an application to a specific machine by way of special hardware or software so that the software will execute only on that machine.54 This is typically accomplished via a hardware serialization scheme. In hardware serialization, when the user installs a software program on a CPU, the program copies the unique serial number of the CPU into itself and thereafter cannot be run on any hardware containing a different serial number. Node-locking can create problems when the licensed node is out of service since the CPU-locked software cannot be easily moved to a back-up CPU.

These problems can be avoided with a token-based scheme or an RS232 25-pin connector. In a token-based scheme, the software program cannot be run unless the original software diskette is inserted in the disk drive of the CPU. This mechanism ensures that the program can only be run in one CPU at a time, but does not "lock" the program to a single designated CPU. Alternatively, a hardware serialization scheme can be used to lock use of a software program to a particular RS232 25-pin connector, which the user can nevertheless move from one CPU to another. Other software suppliers put a serial number in each copy of the software, which

53. The Software Publishers Survey reported that WordPerfect licensed its software on a single machine. However, a more recent publication indicates that WordPerfect may have adopted a compromise between the per CPU and concurrent use licensing approaches. INFOWORLD reported in October 1991, that WordPerfect "took an unexpected tack" when it announced at Comdex that it would offer concurrent use licensing for its PC programs; however, if users choose to copy the program to their local hard disk, they must purchase an additional license. "We ask users to find two numbers — the maximum number of users who would use it concurrently and the number of computers that have it on their local disks — and then license the higher number," reported Pete Peterson, Executive Vice President of WordPerfect. Louise Fickel, WordPerfect Shifts to Concurrent-Use Licensing, INFOWORLD, Oct. 28, 1991, at 1.

instructs the software to check the network to be sure that software with the same serial number is not being used elsewhere. Although this type of serialization allows the software program to be used in alternate or back-up CPUs, it still requires unnecessary use of multiple copies of the program on a LAN. It also does not provide the network administrator with an easy way to find out which user is running a duplicate copy of the software and makes software upgrades difficult because the administrator must install the upgrade with the same serial number on the same computer as the original software.\textsuperscript{55}

Increasingly, per CPU licenses are implemented on LANs through “LAN packs.” LAN packs are typically offered in groups of three, five, or more. For example, a user licenses one copy of software for the server, and then pays an additional amount for each additional copy, or alternatively for the right to copy and use the software for each additional group, or “pack,” of CPUs. The price per unit typically decreases as the size of the pack increases, since the software vendor has no costs for duplicating disks or documentation. Some users dislike license packs because they may be forced to buy more than they need. Jeff Chimbly, LAN services administrator for Farm Bureau Insurance Companies states, “We like to buy [additional copies] in increments of one. Paradox offers increments of five. If you have three nodes, then you have two extra Paradoxes lying around, and that seems like kind of a rip-off.”\textsuperscript{56}

2. \textit{Per User Licensing}. A small number of software suppliers license their programs to an individual, who may be designated by name or by position. This type of license can be enforced on the network through software control or passwords which allow only preauthorized users to access a program. However, this type of software control or password scheme does not work if the user also needs access to the software on a computer at home which is not a part of the network.

Licensing software to an individual makes it clear who is allowed to run the software, but raises other questions. For example, can the licensed user run the software on a second machine without physically removing it from the first machine, and what happens to the license when the licensed user leaves the company or no longer requires access to the software?\textsuperscript{57} Microsoft Corporation has


\textsuperscript{56} Id. at S12.

\textsuperscript{57} Fisher, supra note 52, at 65.
adopted a unique approach to the first of these issues: the "80/20 split policy." If a Microsoft program is licensed to an individual at his place of work, he or she can use the software (without unloading from the primary machine) for up to 20% of the time for use at home or on a portable computer. Similarly, if the program is licensed to an individual at home, he or she can use it at work for up to 20% of the time.58

A LAN alternative to the per user approach is the approach adopted by Swiss Bank, which purchases a license for every single user on the network, including the possibility of simultaneous use. This approach offers an administratively simple way to determine the number of software licenses required at a given network installation, but may be expensive if every network user does not actually require access to the same software products.59

3. Server-Based Licensing. Server-based licensing represents another approach to network licensing. Server-based licenses allow unlimited use of a program on a specific number of servers. In server-based licensing, the "server" portion of an application resides in the server and the "client" portion of the application resides on each node. As a practical matter, the server and client portions of the application could be licensed separately; however, the software supplier typically elects to license the server portion of the program to one or more servers and to permit an unlimited number of copies of the client portion of the program to be made. One of the advantages of server-based licensing is that it is easy to manage. However, since server-based licenses provide for unlimited use of a program on a network with a specified number of servers, they can be too expensive if a company has a need to use a program on only a limited basis. As a result, server-based licensing is more appropriate for programs that are inherently LAN-based, such as electronic mail and other groupware.

A disadvantage of server-based licensing for the software supplier is that server licensing could reduce potential revenue for such programs, since the only limit to the number of users is the speed

58. SOFTWARE PUBLISHERS ASSOCIATION, supra note 31, at 11. According to a recent article, however, Microsoft may be moving to a concurrent licensing approach. Computer World reported that Mike Maples, Vice President of Applications at Microsoft, announced at Comdex in May 1991, that Microsoft had changed its software licensing policy to concurrent use licensing, effective immediately. It is unclear whether this supersedes or supplements Microsoft's earlier, per user approach. Jim Nash, Microsoft Eases LAN Licensing Policy, COMPUTER WORLD, June 3, 1991, at 136.

and capacity of the system, which is constantly increasing due to technology advances. As a result, from the suppliers' viewpoint, server-based licenses make the most sense for disk-intensive software, such as multi-user database managers that limit the number of people who can effectively use a file server because they require more frequent interactions between the local workstations and the database stored on the file server.

4. Site Licensing. Some companies negotiate site licenses for large customer installations on a case-by-case basis. The term “site licensing” has no accepted, consistently applied meaning, and site license terms may therefore vary dramatically. A site license can permit use of software on an unlimited number of computers at one or more geographic sites, it can permit business use by employees of the licensee on an unlimited number of computers at any location, or it can permit use of software on a specified number of computers at one or more geographic sites or at any location. A site license can permit reproduction of the software and/or documentation by the licensee or it can require that the licensee obtain copies of the software and/or documentation from the software supplier. A site license may also enable a licensee to distribute an upgrade by making it available to all nodes via the server rather than requiring the licensee to collect the individual copies of the old version and distribute individual copies of the upgrade, which would be required in a per CPU-based license.

Under a site licensing model, a user typically pays a flat fee for the right to make copies of a software program for use at a particular geographic site. This fee will probably be too expensive if a user requires only limited access to a program. As with server licensing, site licensing is therefore more appropriate for programs that are inherently LAN-based. However, it may be the least popular approach for software suppliers who will be concerned about continuing to use site licenses in network environments because they have no way of knowing how large a network will grow and therefore are required to guess at how much to charge for the site license.

60. For example, Lotus Development Corporation licenses Notes groupware that runs on OS/2 in the server system and on Microsoft's Presentation Manager and Windows on the client workstation, to sites of at least 200 users at a cost of $62,500. Kelly Jackson, Lotus Buys E-Mail, COMMUNICATIONS WEEK, Feb. 18, 1991, at 2.

61. Mort Rosenthal, President of Corporate Software, Inc., a reseller in Canton, Mass., said a software company's size and revenues are factors in site licensing. "The only vendors [selling on an unlimited use license] are the ones desperate for cash," he said, emphasizing the lack of large suppliers who will site license. "This is because it cuts off the revenue stream
As an extra-legal aid to enforcement of a site license, the software supplier may provide the site licensee with a master diskette which contains an internal counter to limit the number of copies made according to the terms of the site license. A similar type of control includes a requirement that the customer copy protect all copies distributed internally, even if the master copy is not copy protected. Where there is no technical limitation on the number of copies, the software supplier may negotiate a contractual right to audit the site licensee’s use to ensure that it does not exceed the scope of the site license. To assist in such a situation, the supplier may require the customer to obtain official labels from the supplier for each copy so that the number of copies reproduced never exceeds the number of labels ordered from the publisher.

5. Concurrent Use Licensing. Most major software suppliers have adopted the concurrent use licensing approach for network software. Concurrent use licensing requires users to pay only for the maximum number of simultaneous uses of the software program on a network. If license manager software is used to enforce concurrent use licensing, users “check out” the software, up to the licensed number of simultaneous uses. When they are finished, they “return” the software, making it available to other users. The benefits of concurrent use licensing include greater flexibility in software use for end users and simplified software distribution for the software supplier since the user can typically increase the number of permitted uses by placing a phone call to the software supplier. It also streamlines distribution of updates, since installation of the update on the file server is typically all that is required to update all users on the network. Finally, it is cheaper than per CPU or per user licensing since the number of concurrent use licenses required will typically be less than the total number of CPUs or users which require access to the program.

One of the disadvantages of concurrent use licensing is that it is virtually impossible to administer without some type of metering system. The most common method today appears to be license manager software, which allows only a specified number of users from the customer once the software is purchased. The only ones who are doing it this way are small vendors and Computer Associates. The only reason to sell site licenses is if you don’t think you’re going to make any other money from the customer or if you’re not the preferred vendor.” Scott Kramer, Vendors, Users, Face Off In Site License Debate, COMPUTERWORLD, June 3, 1991, at 45.

62. SOFTWARE PUBLISHERS ASSOCIATION, supra note 31.
simultaneous access to the software (capacity licensing). Some of these products will allow only a preset number of users to use a program at one time. Other products only audit and report, but do not lock users out. These reports show when the demand exceeds legal supply so that the network administrator can correct the situation by purchasing additional licenses.

Although license manager software utilities are commonly used in the Unix world, many software developers say they are not able to develop an effective license manager program for their applications when running under Windows. This is because in the Windows multitasking environment, an application is counted as being in use when an user retrieves an application and makes it an icon on the screen even if the application is actually not being used.

Some network operating systems include their own license manager software, but each application software program on the LAN must conform to the application programming interface (API) for the license manager software in order to be managed by it. In contrast, the application software program may contain license manager software, but this means that different application programs on the network will use different metering schemes. Network administrators generally want the ability to choose between use of the network license manager software and the application specific metering software. It is therefore desirable if each application program with license manager software checks to see if the network operating system has its own license manager program or if a third party license manager program has been installed. If either exists, the network administrator should be able to turn off the redundant application-specific metering software.

Because of the difficulty of administering a network with multiple license manager software programs, the Microcomputer Managers Association in Warren, N.J., recently published a white paper on network software licensing issues which included a call for an

63. Cheryl Currid, Windows 3.0 - Designed With Networks In Mind, PC WEEK, May 22, 1990, at S44.
65. An example of a network system is the FlexIm system from Highland Software. Software suppliers acquire a logical lock from Highland Software and implement the lock on their source code. FlexIm manages the licenses or "keys." The user licenses FlexIm software along with a rack of key hooks on which to store the license keys. The user buys an application from a software supplier, with a set of keys that define the maximum concurrent usage of the application. A user at any node can access the software as long as a key is available. If additional hooks or keys are needed, the user can purchase them from the software supplier. Flexible License Manager Technical Overview, HIGHLAND SOFTWARE, April 1990.
API which would be common to all network operating systems. Without such a common API, software developers must build multiple metering hooks from their applications into each network operating system's metering program.

After surveying the various license options and the available license manager software, the MMA concluded:

While it is convenient to have the metering software provided with the application, there are problems associated with this approach. First, each application would have its own interface for its metering software. Second, there would be multiple programs which might require that administrative information be entered. It makes much more sense to have a single package provide the metering for all application software on the network.

If we concede this point, however, software publishers have a problem: with which of the metering packages on the market should they be compatible? To overcome this problem, the metering should be done by the NOS ["Network Operating System"]. Users have been clamoring for more and better management features from the NOS for sometime, and metering is just one of the features which must be provided.66

In response to this call, representatives of Digital Equipment Corporation, Microsoft Corporation, Novell Corporation, Highland Software, Inc., microcomputer managers and independent software managers met in December 1991 to discuss a preliminary specification for a proposed API. The draft specification, developed by Digital Equipment Corporation, defined which API calls must be made from an application program to a tracking database or metering utility program. The API would not limit the way an independent software vendor could implement its licenses or metering program because extensions to the metering programs would be allowed, although such extensions could lead to incompatibility among metering utilities.67 One of the issues raised by such a common API, however, is the "dirty metering program." With a common API, the software developer can no longer control the metering program which will be used by the end user to manage the concurrent use licensing. As a result, even one defective, or "dirty," metering program could result in hundreds, or even thousands, of unauthorized

uses. Even worse, a system could be developed using the API to intentionally defeat the concurrent license scheme.

License manager software may also provide other useful information and protection to a network administrator, such as data concerning who has used the various resources on the LAN, how often such resources are used, what time of day they are used, and whether there are times when others are denied access to the resources, which may be helpful in planning future expansion of the network. Some metering systems also include virus protection and security features.68 License manager software may also allow for managing different licensing schemes for different software programs. For example Highland Software Inc.'s network license manager software, Flexlm, can be used to meter concurrent use licensing, but it also allows a network administrator to place reservations on the system for a particular software program. This becomes the equivalent of a single CPU license without the problems of node-locking.69

A license which does not clearly specify the scope of the license granted can have disastrous economic consequences for the software supplier. For example, a supplier who expects each copy of the software to be used on a single CPU will receive significantly less revenue if the license granted permits use of each copy of the software on a single CPU at a time. The pricing model would presumably require a higher per copy royalty for such concurrent use, and the supplier might be unwilling to knowingly permit such use without an appropriate license manager program.

Allocating Liability for Viruses on the LAN

Until recently LANs did not maintain any data of real value to a corporation. With companies downsizing from mainframe computers to LANs, this has changed. Companies are now storing and moving valuable customer files, financial information, payroll, personnel and order entry records over their LANs. The risks posed by computer viruses increase as records move from mainframe computers to LANs.70 As one network manager noted, "In your traditional [information systems] center, you wouldn't allow a stranger to walk in, mount a tape and load programs onto a mainframe. Yet

---

70. Computer viruses are programs that hide within a personal computer and replicate themselves, infecting floppy disks and programs transferred to other PCs.
every day, people carry floppy disks into work and load software onto LAN workstations.” 71

As the number of LANs grows, the number of viruses is also growing. Products less than a year old that search for “over 300 viruses” are almost laughable today. Security specialists cite documentation of more than 1,000 different strains of viruses. The National Computer Association estimates that by the end of 1994, there will be almost 40,000 different virus strains. 72

A study by the Data Processing Management Association found that 26% of the approximately 200 companies surveyed had experienced some kind of virus in January 1990 alone. 73 In December, 1991, Novell sent a letter to approximately 3800 customers, warning them that it had inadvertently allowed a destructive software virus known as “Stoned III,” which can erase or garble everything stored on a hard disk, to invade copies of a Novell software disk shipped that month. 74

Sophisticated computer users are now using a multifaceted approach to computer viruses, which includes updating antivirus software regularly, backing up their records once a week and using virus scanners every time a PC is booted. They are also seeking to protect themselves contractually by including computer virus warranties and indemnities in their license agreements with software suppliers. Software suppliers should not lightly give such warranties, since introduction of a virus to a LAN can result in huge losses. According to John McAfee, President of McAfee & Associates, a Santa Clara antivirus firm, if Stoned III were to get into an organization and spread to 1500 machines, it would cost millions of dollars to clean up. 75 In a real life example of the potential losses which a virus can cause, the Computer Virus Industry Association did a detailed breakdown of costs associated with the virus that struck the federal Internet in November, 1988 and concluded that the virus resulted in $98 million of damages. 76

In addition, it is extremely difficult to determine the origin of a

72. Paul Melka, Wishful Thinking Will Not Make Publicity-Seeking Viruses Go Away, INFOWORLD, April 27, 1992, at 47.
75. Id.
76. Salamone, supra note 71, at 50.
virus, since it can be introduced into a LAN by sharing floppy disks, using bootlegged software, or through dial-out or dial-in access to the LAN. As a result, if the software supplier gives such a warranty, it should require that its licensee be able to demonstrate that supplier's media was the source of the virus.

**Warranting Software In a Networked Environment**

Networks are becoming the lifeline of business as companies move their mission-critical applications to multiplatform networks. Network downtime, the time that the network is either down or degraded, can cause extreme monetary loss, particularly when it affects mission-critical data. In recent studies, major corporations have reported capital losses of astounding magnitude when they have had problems with their networks. One study indicated the average lost productivity resulting from network problems to be in excess of three million dollars per year.\(^7\) Errors, or "bugs," in computer programs which cause minor problems when used on a standalone PC can cause major disruptions in a LAN by destroying shared data files, crashing the network, or producing wrong results which are quickly replicated and relied upon throughout the organization. The frequency of bugs also increases due to the increased complexity of network aware software and the inability of software developers to test their programs on the multitude of possible combinations of hardware and operating system environments which may be found in a LAN. Isolation of the cause of faults on a LAN also becomes difficult as the LAN grows in size and complexity.

The typical warranty included in a shrinkwrap license for prepackaged software does not adequately address the increasingly complicated environment in which the software will be used. It is difficult to imagine that a court will uphold a warranty offered by many suppliers of shrinkwrapped applications, which is limited to defects in the media, when the user is paying thousands of dollars to use the program on multiple nodes. Yet, the software supplier should be hesitant to provide the other typical warranty for shrinkwrapped applications - that the software will perform substantially in accordance with the end user documentation - without clearly specifying the hardware and software environment in which the application will be run. Because a supplier may be forced to spend hours trying to isolate the bug in its software only to discover that the fault has occurred in another component of the network, the

prudent software supplier may wish to include a provision in its warranty that allows it to be compensated at its then current consulting rates for time expended to identify a bug if it is subsequently determined that the reported problem was not caused by the supplier's program. Because destruction of mission-critical data may result in damage to the licensee far in excess of the license fee for its program, the software supplier should also include a disclaimer of any liability for such destruction or loss.

CONCLUSION

This article has attempted to provide a basic understanding of LANs in order to assist in the development of "network aware" licenses which recognize and proactively deal with the movement of software from standalone computers to multiple computers in a networked environment.
APPENDIX

Licensing Methods

1. Per CPU Licensing.

   a. **Single CPU at a time (Use in a LAN is not permitted):** Licensee may use the Software on a single central processing unit at a time. Licensee agrees to treat this Software just like a book, except that Licensee may not rent, lease, or license the Software to others. This means that, like a book, any number of people may use the Software sequentially, and it may be moved freely from one computer to another, so long as there is no possibility of it being used at two different locations at a time. Thus, for example, Licensee cannot share this Software on a local area network. If Licensee wishes to use the Software on more than one computer at a time, Licensee must license such rights from Licensor. Licensee may not electronically transfer the Software from one computer to another over a network.

   b. **Single Designated CPU (Use in a LAN is not permitted):** Licensee may use the Software on a single designated central processing unit [at a designated site] [and in connection with a designated segment of Licensee's business]. "Designated CPU" means the complete equipment listed in Exhibit A hereto or any substituted or backup equipment designated in writing by Licensee and approved by Licensor. Licensee may move the Software to another site which physically replaces the original site upon prior written notice to Licensor [and approval thereof by Licensor]. Licensee agrees to refrain from using the Software on a network or for other sites or premises or on a timeshare or other service basis.

   c. **Single CPU at a time (Use in a LAN is permitted):** Licensee may use the Software on a single central processing unit at a time, except that the Software may be executed from a common disk shared by multiple CPUs provided that one authorized copy of the Software has been licensed from Licensor for each CPU executing the Software. Licensee agrees to treat this Software just like a book, except that Licensee may not rent, lease, or license the Software to others. If the single computer on which Licensee uses the Software is a multiuser system, the license limits use to a single user at a time on that single system. This license allows you to copy the Software over a network for use on a single CPU, provided that the network is only accessible to your organization.

   d. **Single Designated CPU (Use in a LAN is permitted):** Licensee may use the Software on any single personal computer sys-
tem (whether a standard computer or a workstation component of a multi-user network) (the "Designated CPU") and copy the Software solely for the purpose of installing it on the Designated CPU (hard disk or other device), loading the Software into RAM, or creating a backup or archival copy. An alternate CPU may be submitted for the Designated CPU in the event that the Designated CPU becomes inoperable or may replace the Designated CPU, provided that use of the Software on the Designated CPU is terminated and Licensor is immediately notified in writing of the identity and of the successor CPU. Licensee may not copy the related documentation or supporting materials accompanying the Software.

e. Description of Node-Locked Mechanism: Licensor shall provide Licensee with a password corresponding to the equipment Host ID number ("Authorized Equipment") listed on Licensee's purchase order or Licensor's sales order or invoice. This password enables the "Save" feature of the Software when the Software is used on the Authorized Equipment. Otherwise, the "Save" feature is disabled and what shows on the screen may not be stored. If Licensee desires to enable the "Save" feature on other pieces of equipment in addition to the Authorized Equipment, then Licensee may do so by notifying Licensor of the Host ID Number of such equipment and paying to Licensor the amount listed on the then-current price list. Licensor will then provide Licensee with a password which will enable the "Save" feature on such equipment and the list of Authorized Equipment will be accordingly expanded.

2. Per User Licensing.

a. Per User/Single Computer (Use in a LAN is not permitted): Licensee may use the Software on a single computer at a time provided that access to the Software is limited to a single user. Licensee cannot share the Software on a local area network; if more than one user wishes to use the Software or if Licensee wishes to use the Software on a network, Licensee must license such rights from Licensor.

b. Per User (Use in a LAN is permitted): Licensor grants Licensee the right to use one copy of the Software on a single terminal connected to a single computer (i.e. with a single CPU), or on a Licensed Computer Network. A Computer Network is any combination of two or more terminals that are electronically linked and capable of sharing the use of a single software program. A Licensed Computer Network is a computer network for which Licensee has purchased and dedicated at least one (1) Software manual (which...
can include an instruction manual or manuals for the single-user of the Software) for each user of the Software on the network. Each user of the Software must have exclusive access to a Software manual during his use.

c. Per User (Use in a LAN is permitted/Home Use permitted): Licensee may use the Software on a single networked group of computers which share a common disk drive on which the Software is stored, provided that access to the Software is limited to a single user. Provided that each user uses the Software more than 80% of the time on a system located within Licensee's faculty, then that user may also use the Software on a portable and/or home computer.

3. Server-Based Licensing. If this Software is a network version, Licensee may install one copy of the Software on a Network Server for use on a single local area network and may only copy such Software for backup or archival purposes. For purposes of this Agreement, a workstation may include a server. A "Network Server" is a computer managing access to shared resources including files, disks, printers, or other peripherals, used by other workstations connected to the network.

4. Site Licensing. Subject to the terms and conditions of this Agreement, Licensor hereby grants to Licensee the following license and rights:

a. A perpetual, nonexclusive license to use the Software for its own administrative and accounting purposes in the United States on any CPU located at a Site for which the License Fees for the Software have been paid. An alternate Site may be substituted for a Site provided that use of the Software at the original Site is terminated and Licensor is immediately notified in writing of the location of the successor Site. This license does not include the right to download portions of the Software for use on computers located at Remote Access Locations and to provide remote access to the Licensed Software from terminals located at such Remote Access Software [solely for Licensee's internal business purposes]. In the event of an equipment malfunction causing the Software to become inoperable at a Site, Licensee may use the Software at back-up Site on a temporary basis until the malfunction is corrected.

b. Licensee understands and agrees that use of the Software for the purposes of providing data processing services to third parties, such as commercial use in a service bureau or timesharing arrangement, or its transfer to any person or entity outside the country, or its use at any Site other than those Sites for which the
License Fees for the Software have been paid or their successors (other than its use at Remote Access Locations pursuant to subparagraph a. above), is strictly prohibited.

5. Concurrent Use Licensing.

a. Concurrent Use, No Metering Utility Required: Licensee may use the Software on a series of single computers or a single networked group of computers, not to exceed the License Limit purchased. Licensee may physically transfer the Software from one computer to another computer owned or leased by Licensee provided that the maximum number of copies of the software that are used at any one time does not exceed the License Limit.

b. Concurrent Use, Metering Utility Required: Licensee may use the Software on a Licensed Computer Network provided that Licensee has purchased the Server edition of the Software and installed the license manager software program included with the Server edition. A "Computer Network" is any combination of two or more terminals that are electronically linked and capable of sharing a single software program. A "Licensed Computer Network" is a Computer Network on which Licensee has installed the license manager software program. The license manager software program restricts the concurrent use of the Software to the number of licenses which Licensee has purchased. For example, if there are three (3) computers which are concurrently using the Software on the server, then Licensee must purchase a minimum of three concurrent use licenses.

c. Multi-Pack License Grant: A registration number which enables the Software is included, which corresponds to the number ("Number") of concurrent users listed on Licensee's purchase order. If a Number greater than one applies to the Software, and Licensee desires to increase the size of the Number, then Licensee may do so by notifying its place of purchase of the desired Number increase, and paying the applicable purchase price to Licensee's place of purchase. The place of purchase will provide Licensee with a registration number which will effect the Number.

d. Multi-Pack License Grant with License Manager Program: Each single user software package permits one user to access the Software at a time, and each five-pack authorizes five additional simultaneous users. Licensee can increase the number of authorized concurrent users by purchasing additional single-user or five-pack packages. The five-pack comes with an extra disk containing a license manager software program. If Licensee wishes to increase its
user count, Licensee may run the license manager software program and type in the five-count serial number allotted with the five-pack. The five-pack can be installed only in a network shared hard disk, and it operates only in conjunction with an installed single user package. Licensee cannot operate the five-pack by itself.

**COMPUTER VIRUS PROVISIONS**

1. **Definition of Computer Virus:** A "Computer Virus" is an undocumented and unauthorized program designed to cause loss of, or damage to, data files; or gain access to, and/or interfere with, the operation of, other programs or computer resources, or any other results not intended by the user of the computer system on which the virus program resides.

2. **Computer Virus Warranty:** Licensor represents and warrants that there are no Computer Viruses in the software.

3. **Computer Virus Screening Provision:** Licensor shall use due diligence in screening all Software to be delivered to Licensee in order to minimize the possibility of the introduction of a Computer Virus. If Licensor fails to perform such screening with the result that an identified and acknowledged Computer Virus is introduced into the Licensee's systems, Licensor shall be responsible for any loss, damage or liability caused by such Computer Virus. If Licensor performs such screening, but a new or unidentified Computer Virus is nevertheless introduced into Licensee's systems through Licensor's Software, Licensor shall only be liable for the value of the Software that Licensor supplied.

4. **Computer Virus Screening Provision and Disclaimer of Computer Virus Warranty:** The parties acknowledge the need to cooperate to reduce the risk that a Computer Virus will be introduced into Licensee's computing environment on media supplied by Licensor. Licensor agrees to use a commercially-available anti-virus screening program to screen all media containing the Software before such media are delivered to Licensee. Licensee acknowledges that Licensor does not represent or warrant that the media delivered by Licensor will be Computer Virus-free. Licensee agrees to employ a commercially available anti-virus screening program to screen all media delivered by Licensor to Licensee. Licensor's sole liability, if Licensee's screening procedure detects a Computer Virus or such media or if Licensee is otherwise able to demonstrate that media supplied by Licensor is the source of a Computer Virus introduced into Licensee's computing environment, will be to deliver
new copies of the Software on media free of the identified Computer Virus, at no charge to Licensee.

Network Aware Warranty

Express Warranty: Licensor warrants that the Software will perform substantially in accordance with the published documentation for such Software (the “Documentation”), only when operated on or in conjunction with the hardware and software with which the Software was designed to be used as described in the Documentation, during the ninety (90) day period following delivery of the Software Licensee (the “Warranty Period”).

Exclusive Remedies: Licensee’s exclusive remedy, and Licensor’s entire liability in contract, tort or otherwise, shall be to use its best efforts to provide a correction or workaround for any substantial nonconformity of the Software with the Documentation (“Error”) which is (a) reported to Licensor by Licensee during the Warranty Period and (b) reproducible by Licensor in the execution environment. If, however, after repeated efforts, Licensor is unable to provide a correction or workaround for any reported Error, then Licensee’s exclusive remedy and Licensor’s entire liability in contract, tort, or otherwise shall be for licensor to refund the amounts paid by Licensee for the Software upon Licensee’s return of the original and all copies of the Software in its possession, together with its certification that it has ceased all use and distribution of the Software.

Exceptions from Warranty: The warranties set forth above shall not apply to any defects or problems caused in whole or in part by (i) any defect in any portion of any hardware or equipment, (ii) the failure of any portion of any hardware or software to function in accordance with applicable manufacturer’s specifications, (iii) any modification or enhancement to the Software by Licensee or any third person or entity other than Licensor; (iv) the failure of Licensee or any third person or entity to follow the most current instructions promulgated by Licensor from time to time with respect to the Software; or (v) the negligence of Licensee or any other third party or entity. Licensor shall not be responsible in any manner for errors or failures in proprietary systems, hardware or software other than those of Licensor. It is Licensee’s responsibility to maintain backup data to be able to regenerate or duplicate data in the event of loss. In the event that Licensor determines that any warranty claim reported by Licensee falls within any of the forego-
ing exceptions, Licensee shall pay Licensor for its services at Licensor's hourly rates than in effect.

**Disclaimer of Express or Implied Warranties:** EXCEPT FOR THE EXPRESS WARRANTIES STATED IN THIS AGREEMENT, LICENSOR MAKES NO ADDITIONAL WARRANTIES EXPRESS, IMPLIED OR STATUTORY, AS TO ANY MATTER WHATSOEVER. IN PARTICULAR, ANY AND ALL WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS ARE EXPRESSLY EXCLUDED. LICENSOR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE.