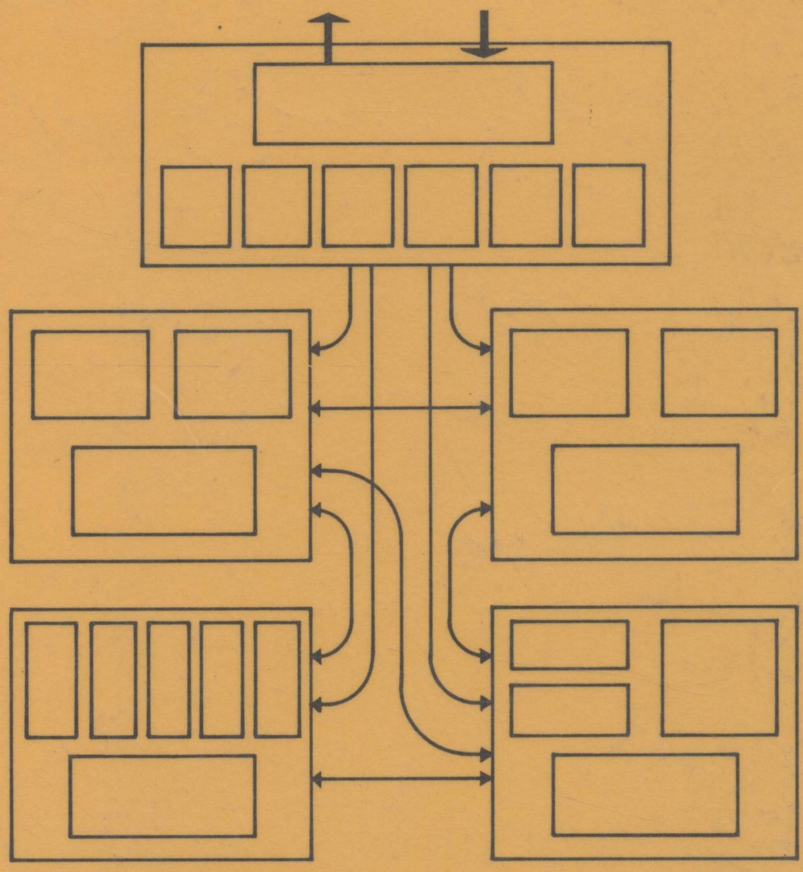
The PC LAN Software Report

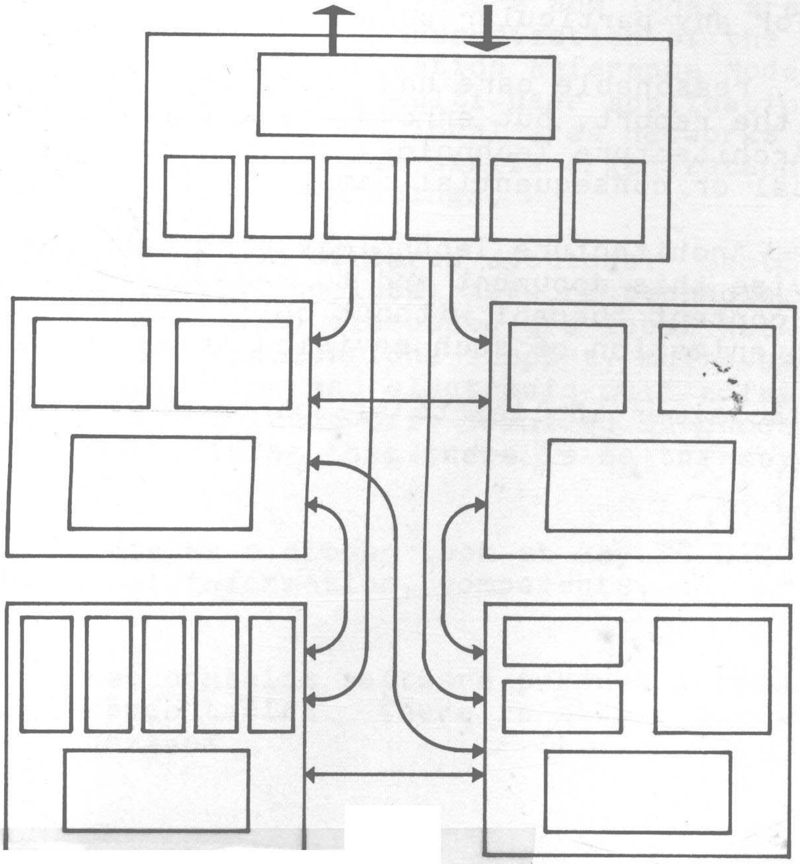


ARCHITECTURE
TECHNOLOGY
CORPORATION
SPECIALISTS IN COMPUTER ARCHITECTURE

P.O. BOX 24344 • MINNEAPOLIS, MINNESOTA 55424 • (612) 935-2035

The PC LAN Software Report

October 1985



ARCHITECTURE
TECHNOLOGY
CORPORATION
SPECIALISTS IN COMPUTER ARCHITECTURE

P.O. BOX 24344 • MINNEAPOLIS, MINNESOTA 55424 • (612) 935-2035

DISCLAIMER

Architecture Technology Corporation makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

Further, reasonable care has been taken to insure the accuracy of the report, but errors and omissions could have occurred. Architecture Technology assumes no responsibility for any incidental or consequential damages caused thereby.

Further, Architecture Technology Corporation reserves the right to revise this document and to make changes from time to time in the content thereof without obligation to notify any person or organization of such revision or changes.

This disclaimer applies to all parts of this document.

Foreword

There are over sixty original equipment manufacturers of local area networks for personal computers, and it seems as though each day a vendor is introducing a new local network product. Unfortunately, not all of these systems are compatible. The sophisticated users who are growing into multi-user applications on local area networks and need these resources to perform their jobs effectively are faced with a lot of choices.

With the explosive growth of local area networks, several major trends are emerging: there are now local area network operating systems; there is standardization of the International Standards Organization Reference Model high level protocols in vendor products; multi-user applications are being built on top of databases; and local area networks are expanding their scope from departments in single organizations to diverse organizations in multiple buildings.

This report consists of three sections. Section one includes an introduction to local network technology and software in hardware systems. Also discussed are local network operating systems, servers and applications support, multi-user databases, and multi-user accounting and electronic mail software. Many of the considerations and trade-offs involved in choosing a system are addressed, emphasizing that there is no turnkey solution for networking needs.

Section two takes a closer look at key PC LAN software systems. Technical information, components, and pricing are included.

Section three contains software product information compiled into quick reference tables. There is also a complete listing of the vendors' addresses.

Table of Contents

Section I: Introduction to the Technology

Section II: A Closer Look at the Key Products

Section III: Supplemental Information

List of Figures

Section I

Section II

List of Tables

Section I

Section II

1. Introduction to PC Local Network Technology

Since this report is intended to provide in-depth knowledge of personal computer local area network software (PC LAN software), this introduction is provided to give a quick, general overview of PC LAN technology.

1.1. Overview

1.1.1. No Turnkey Solution

Despite what many vendors of local area networks claim, there are no plug-in-the-wall solutions to networking problems. There are over 60 OEM vendors of local area networks for personal computers, and this means there are over 60 different generally incompatible systems. Of these systems, at least 20 are for one machine--the IBM PC. Even these sytems are incompatible with each other. But there is a lot more to implementing a PC LAN than buying and installing hardware. This report will look at the software aspect in depth, as well as long term considerations. Thus, at the present time there is no such thing as a turnkey solution for determining the right LAN for a PC environment.

1.1.2. Components of a LAN

PC LANs consist of three major components: hardware, software, and people. Hardware includes the personal computer (PC) machines and a network interface card that connects the PCs into a local area network. The PC may or may not include floppy disks since one trend in PC LANs is diskless PCs. They eliminate some of the costs of using floppy disks and, to a degree, enhance security as large amounts of data can not be taken off the system via floppy disk. Typically, most systems require extra RAM in the PCs because this is where the LAN communications software will reside. However, RAM requirements can vary extensively from system to system, anywhere from 16K to 128K.

Software should be able to support single and multi-user applications although it may require some extension or modification for a multi-user LAN environment. Support for future software applications must be considered when choosing a LAN. Software also consists of utilities which perform network commands.

The third component of a PC local network system is people, the "hidden cost." People must install the cable, connect the PCs, configure the software, and bring up the system. They must manage and maintain the system and train others how to use it. Although these things may be easy to do with four or five computers, when a system grows to sixty or one hundred PCs on a

LAN, a management problem may result as many shared resources are distributed.

1.1.3. Benefits of PC LANs

PC LANs offer several benefits. They have a very low cost per user. If the PC LAN is carefully planned and installed, the system can actually bring a lower cost per user than a stand-alone PC environment. Floppiless PCs and shared resources which take advantage of economies of scale, such as large hard disks, help keep costs down.

A LAN provides smooth system growth as adding a PC to a LAN is very easy: just plug an adapter board into the expansion slot and tap onto the cable. Since the CPU is inside the PC, there is constant power per user. In contrast, in a mini or mainframe computer environment, adding a terminal to a host environment decreases someone else's computer power. However, one thing that varies in a LAN is the amount of input/output (I/O) available per user.

LAN systems are very flexible and versatile. For example, they can be used for word processing at one time, spreadsheet analysis at another, and perhaps batch updating to a database overnight. In addition to acting as workstations, PCs can also be used as servers for sharing peripherals.

1.1.4. Disadvantages of LANs

Despite all of these benefits, there are also disadvantages to PC LANs. Software complexity increases substantially in a LAN environment where there are multiple PCs, multiple users, and multiple applications.

This complex, multi-user situation creates an environment in which it is very difficult to locate the source of a problem when it occurs in a system. Although a problem may appear to be similar to one experienced with a PC in a stand-alone environment (for example, the screen goes blank, the printer won't print, there is no response), the problem may no longer be with the machine but with the LAN. Perhaps the network interface went bad, someone disconnected a cable, or a server failed. For this and other reasons, some unique expertise is needed to design and develop LAN systems, expertise far beyond that of people who install PCs. This expertise demands an understanding of multi-user environments, allocation of resources, and communication technology.

1.2. Topologies and Other Issues

1.2.1. Generic Topologies

There are several generic topologies used in local area networks. These include the star, ring/loop, bus and irregular topologies.

The star topology consists of a center switch and nodes, or PCs. The idea behind this topology is that all communications go through the center switch. Sometimes PC LANs with star topologies share resources at the center switch, but this is not always the case. There is no reason why a PC in one location can not share a disk with a PC in another location.

In the ring or loop system, the switch is distributed. Typically, there is a switch in each personal computer attached to the network, though, there may be couple of nodes sharing one switch. But for the most part, there is one node or PC that has its own switch and attaches to the RAM.

In the bus topology the switch is distributed. The packet is broadcast throughout the system until a node receives it.

Irregular topologies aren't used very often in PC LANs. This topology is more popular for mini and mainframe computer environments where there are redundant point-to-point links between machines.

1.2.2. Carrier Sense Multiple Access--CSMA

A contention channel is the basis for CSMA, Carrier Sense Multiple Access. With CSMA, users are sharing one channel and contending for access to that channel. The idea is to implement a "listen before send" CSMA protocol.

For example, suppose "A" wants to broadcast a packet intended for PC "C". "A" listens for activity on the bus; there is no activity, so "A" sends out the packet, and "C" receives it. The bus is then idle for awhile. Then "B" comes along, sends off a packet, and "C" receives that packet. But something interesting happens when a third packet is sent. "A" sends out his packet, and then "B" seems to jump on and cause a collision or garbling of data. Why did "B" Jump on to the system when it should have listened before sending its packet?

This problem occurs due to propagation delays in the cable. Most of the contention channel networks run anywhere from one to ten million bits per second (one megabit per second or 1 Mbps). These very short delays in the system are very critical. When there are thousands of feet of cable in a system, one node may start to transmit at one end; however, if the node at the other end has not sensed this, it will decide to go ahead and transmit a packet--and a collision occurs. For this reason, a CSMA system is sometimes referred to as a distance sensitive protocol.

1.2.3. CSMA with Collision Detection

With Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the system should detect whether a collision may occur and retransmit the packet.

There are several advantages to CSMA/CD. It is very simple to implement. Also, there is no single point of failure; it is a totally distributed technique. There's no master/slave polling scheme and no token being passed around. CSMA is also well understood, measured and simulated as it has been in systems since the early 1970s.

However, there are several disadvantages to CSMA/CD. It's not deterministic; an upper bound or guarantee can't be made on how long it will take to pass a piece of information between two nodes due to the random-access nature of CSMA and the possibility of a collision. This is undesirable for a process control environment. Although the time needed to pass information between two nodes is very small, in a process control environment it is very critical. If no guarantee can be made regarding this time interval, then it is not deterministic.

There is also no guaranteed delivery of data. If the receiving node of the PC is turned off or busy, there is no way for the user to know if the data packets reached the receiving node, especially at a very low level in CSMA.

Because of the distance sensitive nature of CSMA, it tends to be topology dependent. Most CSMA systems are based on bus topologies. CSMA also tends to break down under very heavy loads, although this is not really a major disadvantage for a typical PC environment.

1.2.4. Token Passing

In a token passing system, there is something called a free token, which is basically a small packet, a pre-defined bit pattern of ones and zeros that circulates around a ring.

As the the free token circulates around the system, each node examines it. The node can then do one of two things: it can either pass the token to its neighbor, or it can append data to that token and send out a data packet. For example, "A" decides to send some data to "C", so "A" grabs the free token, appends data, creates a data packet, and sends it out over the network to "C". Eventually, it comes around again, and "A" generates the free token and passes it onto "C".

A token passing system allows nodes to send multiple packets before giving up the token. However, a totally fair access scheme must only allow the station to send one packet of some maximum size and then pass on the token. Then the station will have to wait until the token comes around again before it can send out the next packet, and so on. But, a priority system could be implemented: different packet sizes could be assigned for the stations, and the stations could have multiple passes at the token before they give it up.

There are several advantages to token passing. Token passing is a deterministic protocol. This means the user determines how long it will take for another opportunity to use a token. This enables the user to put an upper bound, a worst case response time, or a token passing time on the system. There is also guaranteed delivery by acknowledgment bits as the packet circulates through a receiving node. With token passing, the system is not distance, speed, or topology dependent, and the system is always stable.

Token passing schemes also have some disadvantages. They are more complex as all nodes must examine the token and determine whether or not they want to send data packets. Also, there is the possibility that a PC could lose or replicate tokens. Another problem is that nodes may become points of failure, especially if a PC is turned off.

1.2.5. Protocols

Protocols are simply a set of conventions that allow two or more end points to communicate. There are essentially three elements in protocols: syntax, semantics, and timing. The syntax of a protocol defines the fields; for example, there may be a 16-byte field for the addresses, a 32-byte field for check sums, and 512 bytes per packet. The semantics of the protocol attach meanings to those fields. For example, if an address field consists of all ones, it is a broadcast packet. Timing, the number of bits per second at which data is sent, is also important, not only at very low levels of protocols but at high levels of protocols as well.

Figure I-1 illustrates a diagram of a typical message format. At the beginning of the message, which is flowing one way over the network, some kind of synchronization characters can be assigned so that another node on the network can see that the message is coming and synchronize its receiver with the sender. The message header contains addressing information--where the message is going and where it comes from. The message text itself is information which is going to be sent over the network. It has a header and in some instances a trailer, which is an indication of where the message ends. There may be control and synchronization characters at the end of the message too.

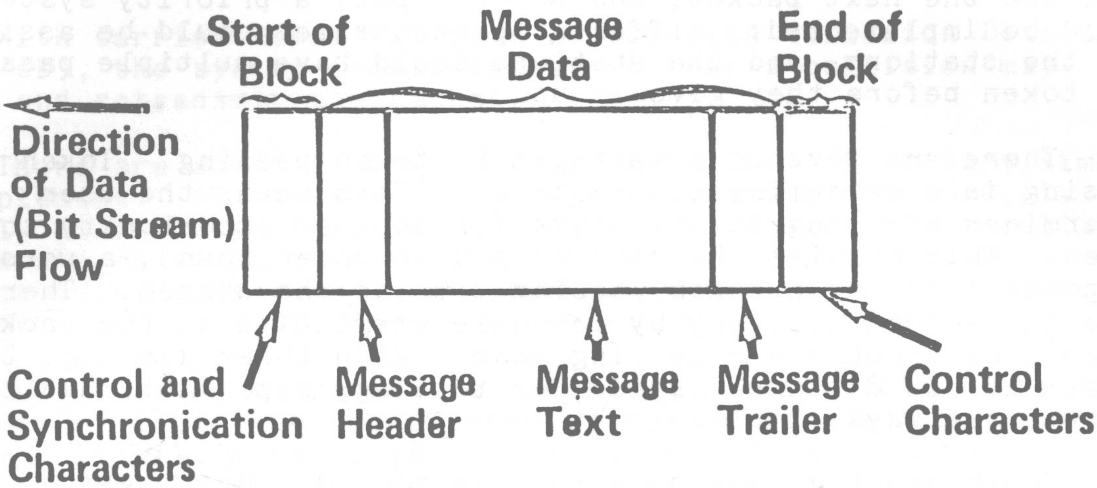


Figure I-1: Typical Message Format

There are several considerations for end-to-end protocols. One issue is addressing structure: will it be flat so that there is one large addressing space for an interconnected system, or will it be heirarchical so that there is a tree-like structure of addresses such as network, station, and socket within a station? What is the addressing space of the system--how many nodes, or PCs, can logically be addressed on the system? Despite what many vendors claim, the number of PCs that can be attached to a system is typically far less than the addressing space. What should the data unit size be? There must be a compromise between large and small data unit sizes as large units may "hog" the system and small units may have more overhead. Does the system have some type of error control? If something goes wrong, can the protocol system indicate what the problem is, and does it provide for error recovery? How do packets synchronize themselves in the protocol layers? Suppose someone inadvertently affects someone else's data packet or writes into the wrong file server, is protection provided? Is there protocol monitoring for resource management and performance analysis of the system?

1.3. ISO OSI Reference Model

1.3.1. Layers of Protocol

The concept of layering is addressed by the International Standards Organization (ISO), which produced what it calls the reference model for Open Systems Interconnections (OSI). This is the ISO OSI Reference Model, as shown in Figure I-2.

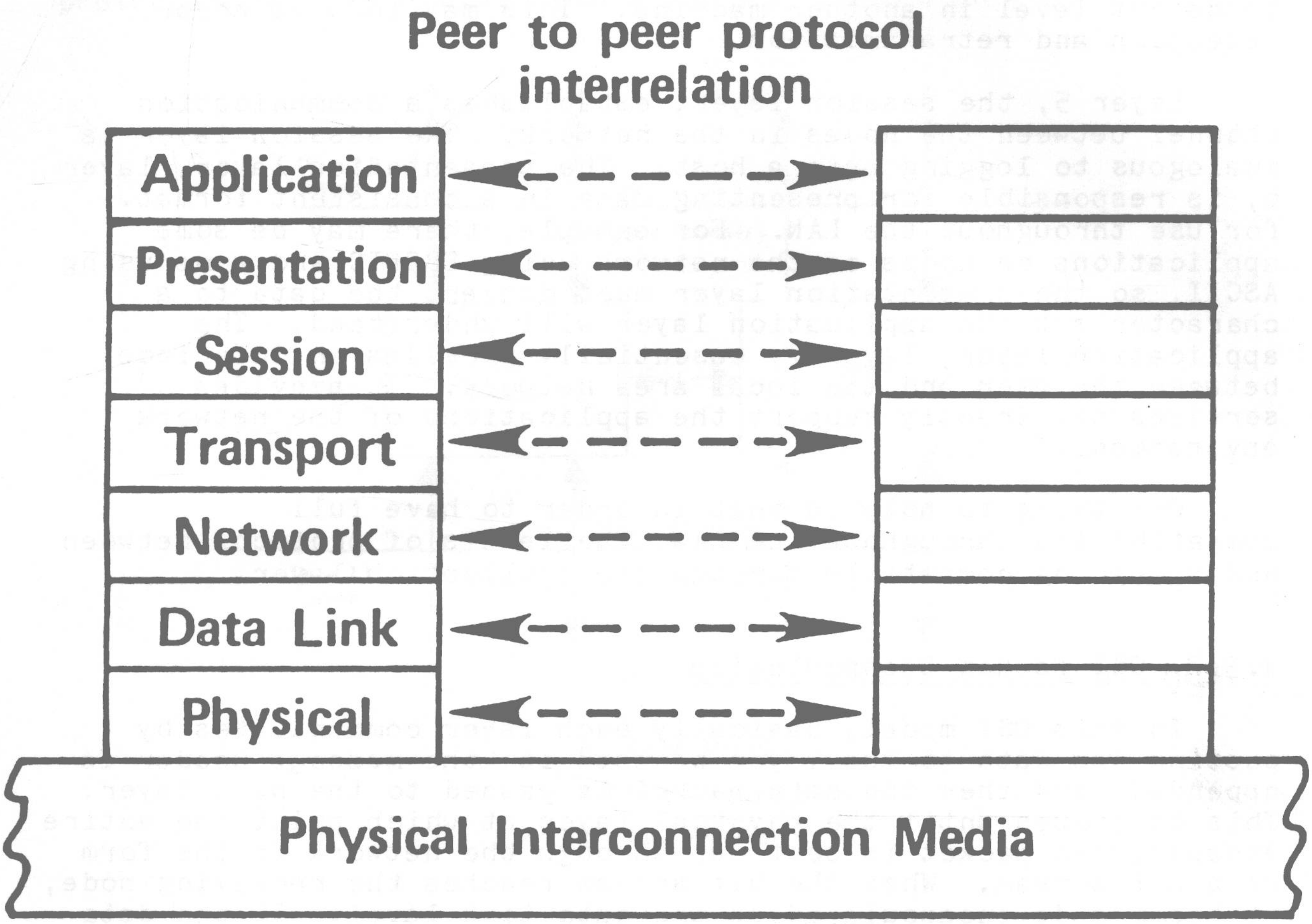


Figure I-2: ISO Seven-Layer Reference Model

Basically, the model depicts seven stratified layers of protocol. The physical level, level 1, is the lowest layer. This layer sends and receives bits in the layers across the network. The next layer, the data link level, is where the bit stream is defined. This level contains the access and control mechanism. While much can be done using hardware in the data link layer, several systems currently exist which actually use software even as low as the data link level. There is a lot of activity with Very Large Scale Integration (VLSI) used to control this level.

The network layer, level 3, is responsible for routing and switching data throughout the network. However, not all PC LAN systems have network levels of protocol. The end-to-end