THE STACK

****

Volume.7 No.9 SEPTEMBER 1983

OFFICIAL NEWSLETTER OF
THE LONG ISLAND COMPUTER ASSOCIATION, INC.

****

President's Message

I

This organization has grown to be one of the largest and most active of its kind in the world. We have formed new special interest groups frequently as interest has grown in specific hardware, software, and applications. It has nonetheless remained a continuing source of frustration that so few of our members are users of Apple computers, and that those who are use their Model II's, II Plus's, and IIe's as second or third machines, and then primarily for game playing or for special applications only.

We have discovered that there are several readily-available Z-80 cards which permit Apple computers to utilize both CP/M 2.2 and CP/M Plus, and that many Apple users have, or contemplate getting such cards. Unfortunately, we have also found that not all Apple users have serial data transmission capability, and those that do often do not have data transfer programs compatible with the protocols of XMODEM (the de-facto standard among RCPM users).

Well, there is a very fine series of files including a short boot program, documentation, and source code for the APMODEM system. This is public domain material, but it works better than many commercially-available systems. Let us know who you are, Apple users, join LICA, and this software is yours. By the way, our CPMUG-SIG/M group has well over 150 volumes of public domain material, much of which will run on your Apples. Isn't this what an organization such as ours is all about?

II

There will be some changes in our traditional scheduling beginning this month. Due to conflicts with the High Holy Days, both our IBM PC meeting at the Commack Campus, and the several second-Friday meetings at the Old Westbury Campus of NYIT will be cancelled. Our General Membership Meeting, usually held on the third Friday will be held one week later, on September 23rd.

Beginning with October, there will be an IBM PC meeting at Old Westbury on the First Friday. Our traditional special interest group meetings will resume at their established times.

The success of our experiment in July, wherein we instituted multiple simultaneous seminars has occasioned the need to know much further in advance just who would like to speak. Contact Al Levy or me as soon as you can offer us a firm commitment.

For example, in October both Ron Richards, the remarkable speaker on rotating media who captivated us twice last year with his ability to make the complex truly understandable, and Angela Coble of Data Access Systems, Inc., the terminal refurbisher and vendor, will join us. A beginners group will meet at this and most General Meetings. Remember - we were all beginners once!

III

A nominating committee has been formed to search for an appropriate slate of officers for this Corporation during the calendar year 1984. Those wishing to volunteer their sevices or to suggest nominees are urged to contact Dave Schwartz.

Al Levy has begun the formation of subcommittees to solve the many logistical problems inherent in planning an Indoor 1984 LICA Computer Faire #3. Based upon the experience of other computer hobbyist organizations, which experienced a ten-fold growth in activity from the time of their first to their second Fair/Faire/Flea Market/Bourse, we can reasonably expect to double our volume in both exhibitors and attendees on the first Saturday in June next year. We need you to volunteer NOW.

IV

Finally, on a personal note: many persons obtain The STACK through retail computer stores or borrow copies from their friends. Please remember that LICA is a voluntary associaion, and that each of us has other obligations to ourselves and to our families. While we feel very strongly our obligation to respond to sincere requests for information and assistance, we think it not unfair to insist on two points. First, please restrict your calls to reasonable evening hours during the work week, and to afternoon hours on weekends and holidays. Secondly, while we'll never refuse to supply the requested aid and assistance, we do ask that you send in your $12 annual membership fee, so that we can continue to produce the many tangible services of our organization, including this remarkable publication. Thanks a lot. Al Stone

SECRETARY'S REPORT ON LICA MEETING OF 19 AUGUST 1983

Al Stone, our president, announced that the Sept meeting of LICA would take place on 23 Sept, (the fourth Friday of the month rather than the third Friday) because of religious holidays.

Mrs. Feinstein, of Right On Programs in Huntington, (516) 271-3177 announced that they are looking for programmers for educational software, especially for the Apple and other popular computers.

Al Levy discussed plans for the 1984 LICA Computer Fair. He asked for five volunteers to search for possible locations for the fair so that he can report in Sept. He received a good response.

****

Because of the general interest in the subjects of the two speakers scheduled for the evening, it was decided not to split into separate groups as was done at the previous meeting.

The first speaker was **Andy Konig** of Bell Telephone Laboratories who spoke on the **UNIX** Operating System.

Andy began his talk with a review of the history of multi-user time-sharing systems leading to the development of UNIX. He described the specific characteristics of the system such as its portability, redirection and pipelining.

In simple words, redirection refers to the ability of the operator at run time to decide where the program output should go to, i.e. any available IO device or another file. Pipelining is the procedure of having the output data of one file serve as the input data to another file.

Files are treated as just a string of bytes and can be read from or written to anywhere. Files are named hierarchically so that a large number of files can be used with easy and direct access to any of them. There are extensive commands for file manipulation (including the ability to erase another user's file).

Processing is very versatile, such as the "fork" procedure, i.e. to generate additional copies of processing code so that two or more concurrent operations can proceed.

The UNIX Shell is the command processor which interfaces with the user.

Various applications of the UNIX system were described.

Andy gave a very informative talk and it was warmly received by the large audience.

****

The second speaker was **Thomas Golway** of Control Information Systems who spoke on Local Networks.

Local Networks such as Ethernet are used generally for data communication in the order of 1-3 kM with typically 10 Megabaud rates. Some go up to 50 Megabaud and it is expected that the introduction of fiber optics will allow even higher rates.

Tom discussed the technical and operational characteristics of these networks for use in message transmission and switching. He described the different commercial data and communication systems, the type of equipment used and the nature of the problems encountered.

The LICA audience was introduced to a world of data operations which was far removed from ordinary home computers, but which was interesting to learn about.

Frank Davidoff, secretary

FALCON COMPUTERS

MON - WED 9 - 5 -
THUR/FRI 9 - 9 - SAT. 10 - 5

VISA · master charge

SALES • SERVICE • SOFTWARE • SUPPLIES

FRANKLIN ACE PRO (APPLE II ®) COMPATIBLE

The Professional Personal Computer System

FRANKLIN COMPUTER CORPORATION

$1,595 MFG. LIST

*** ACE PRO Includes**
- ACE 1000 64 K Color Computer
- ACE 10 Floppy Disk Drive
- ACE Display 80 - Column Card
- ACE Writer II Word Processing Program
- ACECalc Spreadsheet Analysis Program

FRANKLIN ACE 1000™

FALCON'S COMPLETE TURNKEY SYSTEM

• ACE PRO Package*	$1,595.00
• Gemini - 10 X Dot Matrix Printer	$399.00
• STARGRAPH, Graphics Interface Card	$99.00
• NEC, 12" Green Monitor	$149.00

Special $1,849.00 Suggested List ~~$2,242.00~~

$99.00 MO., 2 YR. LEASE, PURCHASE • AUTHORIZED SALES AND SERVICE

FRANKLIN ACE IS A TRADE MARK OF FRANKLIN COMPUTER CORP. • APPLE IS A REGISTERED TRADE MARK OF APPLE COMPUTER INC.

SUMMER CLEARANCE

ALTOS SERIES 5, MP/M, 3 user, Select Word Processor, Multiplan, and Wyse 100 Smart Terminal	$ 3,295.00
NEC PC-8001, Expansion interface, Dual 5 1/4" Drive, Hi-Res green monitor, includes software: CP/M, Select W.P. w/dictionary, and File-Fax data base	$ 1,595.00
NEC PC-6000 Computer with Canyon Climber & Shamus Software	$ 299.00
Atari 400 Computer	$ 139.00
Atari 1200 Computer	$ 495.00
Commodore VIC-20 Computer	$ 139.00
Commodore C-64 Computer	$ 239.00

FRANKLIN and APPLE II PERIPHERALS

ALS Z-Card CP/M	$ 136.00
ALS Condor I DBMS	$ 149.00
ALS 64K CP/M (3.0) Card	$ 299.00
ALS Smarterm 80 Column Card	$ 249.00
Microsoft Softcard CP/M	$ 233.00
Synetix 294K Dual RAM Disk	$ 595.00
Franklin/Apple Joy Sticks	$ 24.00
Echo II Speech Synthesizer	$ 99.00
Roland Compu Music System	$ 349.00

FALCON 938-8844
COMPUTER CORPORATION
105 N BROADWAY, HICKSVILLE 2 BLOCKS SOUTH OF SEARS

VICTOR®

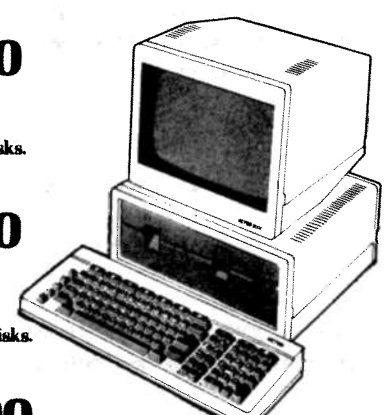
The intelligent choice

One look at the prices and capacities of these three popular Victor 9000 configurations and you'll understand why the Victor has quickly become the world's 2nd most popular advanced 16-bit microcomputer.

The Victor 9000 quite simply offers the best price/performance combination available on the market today.

The powerful memory and storage capacities of the Victor 9000 are only part of the Victor performance story.

Designed to be a hardworking, hands-on computer, the Victor 9000 gives new meaning to the term "user-friendly." From the human size, detached keyboard to the tilting, turning, high resolution display screen, the Victor 9000 makes complex business computing easy. And with scores of proven business application software packages available right now, plus networking, complete communications capabilities, and a complete line of high performance peripherals, the Victor 9000 is the class of its class.



$3,995.00
The 16-bit Victor 9000 Personal Business Computer with two single-sided floppy disks.

$4,745.00
The 16-bit Victor 9000 Personal Business Computer with two double-sided floppy disks.

$5,995.00
The 16-bit Victor 9000 Personal Business Computer with internal hard disk.

Mfg. List Shown
DISCOUNTS AVAILABLE

SYNPAD-A NEW CODE FOR ULTRA-HIGH SECURITY

Jack Schacter

On June 21, 1957, the highest ranking Russian spy ever to be captured by the F.B.I., Rudolf Abel, was arrested in New York City. He was later to be traded for Gary Powers, the U-2 pilot who was shot down flying over the U.S.S.R. What made this event of real interest to our cryptanalysts (codebreakers) was the discovery of an unbreakable code when Abel's room was searched. The code was in the form of a tiny booklet hidden in a block of wood found secreted in a wastebasket.

Abel had been using a "One-Time Pad" to communicate with Moscow because it was absolutely safe. A "One-Time Pad" consists of a series of random digits arranged in a table. To use it, the message is first converted to numerical form. For example: A=01,B=02,....Z=26, etc. Then the numbers in the "Pad" are added to those in the message. The result is the coded text. The numbers used are then crossed off and never used again, hence the name "One-Time Pad".

This code (technically a cipher because it deals with letters rather than words) is unbreakable because each letter is encoded in an unpredictable way. The basis of codebreaking is to find a pattern of some sort in the encoded message and use that to develop a decoding algorithm, hopefully the same algorithm being used by the intended receiver. In the case of the One-Time Pad, the letter "e", for example, would be encoded by one number one time and by another the next. There is no pattern because the encoding table has been deliberately chosen so as to have no relationship among its digits. As a result, this code cannot be cracked.

The obvious question is: "Why hasn't the "One-Time Pad" superseded all other coding schemes since it has been known for over half a century and is absolutely secure ?".

The answer is that it has three substantial disadvantages:

1. A physical object, the pad, must be kept in order to code or decode. There is no way that the scheme can be memorized except for perhaps one or two short messages.

2. This physical object must be kept hidden because any finder would be able to decode and perhaps code messages.

3. The length of the pad must be short, so as to keep the pad small and concealable, thus ultimately requiring replacement, or, at least limiting the length or number of the messages.

These problems could be overcome if there were an easily memorizable formula for generating the pad. Unfortunately, the existence of such a formula would violate the condition that the numbers on the pad be random. Theoretically, therefore, a formula is unattainable. Practically, however, there is a solution. What we shall do here is to develop an algorithm that we call "Synpad" that can synthesize a One-Time Pad so closely that no method is known to exist that can distinguish them.

Secure Commercial Communication

The purpose here is not to develop a code for spies, but rather a secure method of communications between people or businesses, such as banks in the transmission of wired money transfers, or in the keeping of secure data. We shall call this new code Synpad. The name is short for "Synthetic One-Time Pad".

Synpad is superior to DES (the government's data encryption standard) because its basic algorithm can easily be memorized, the encoding and decoding processes are suitable for a microcomputer, and there is no doubt about NSA having left a trap door solution in it somewhere or having a specially designed computer fast enough to break it.

SYNPAD-A NEW CODE FOR ULTRA-HIGH SECURITY-Jack Schacter

Normal Numbers

Synpad depends on the mathematical concept of "normal" numbers. Every real number can be expressed as an integer plus a decimal of infinite length. A whole number is considered to have a decimal part consisting of an infinite number of zeroes. A normal number is one in which any combination of a fixed number of digits is equally likely to be found. For example, a normal number contains an equal number of each digit from 0 to 9, the two group combinations 00 to 99, the three group combinations 000 to 999, etc. In other words, it behaves as if it were composed of equally likely, independent digits or groups of digits.

It has been shown that "almost all" numbers are normal. At first, this appears to be a strange result because most of the numbers we deal with are definitely not normal. Even a non-terminating decimal for a fraction like 1/3 contains only 3's so it cannot be normal. But, most numbers are not rational. In fact, irrational numbers are so much more frequent than rationals, that all the rational numbers between 0 and 1 represent only a vanishingly small proportion of the total. Irrational numbers, such as the square root of two, the sine of twelve degrees, pi, log 3, etc., consist of an integer part and a non-terminating fraction. It can be mathematically proven that the decimal portion does not repeat as it does for a fraction like 1/3 or 1/7.

It is exceedingly difficult to prove that a given number is normal. It is strongly suspected that all irrational roots of algebraic equations, such as the square root of 2, and all transcendental numbers such as pi or sin(22), are normal. One of the reasons that pi has been calculated to millions of decimal places is to test for normality. Thus far all tests have been positive.

Basis of Synpad

Suppose we had an irrational number and from somewhere in it we selected 100 digits in sequence. We could then use these digits as if they were a One-Time Pad. If we wanted more numbers we would need only to continue to calculate them. This is the basis of Synpad.

But, one could say, there is a formula for generating these numbers therefore there must be a pattern that can be used to break the code. However, it is easy to show that there is no such pattern. Suppose we gave the 100 digits that we have selected to the cryptanalyst. Even with this help, he could not determine what the next digit is going to be unless he knew which irrational number was being used and where in this number we are picking digits. And if we gave him a thousand or a billion digits it would not be of any more help in predicting the next digit. This is true because in any normal number all groups are equally likely to occur. Therefore, this group could have come from any of an infinite number of places in any of an infinite number of normal numbers. Since the number that the group came from cannot be determined, the next digit is not predictable. This, of course, makes the prediction of a pattern unattainable. As a result, any code breaking procedure must be based on an exhaustive test of all possible numbers. If the number of combinations to be tested is made sufficiently large, the time required to do the code breaking may be caused to be as large as desired.

One result of using this method is that even if the cryptanalyst has been given both the clear and coded texts of a message, this is of no help in decoding the next message no matter how much captured material is available.

Calculating an Irrational Number

Irrational numbers may be calculated to any number of significant figures by several methods. We learned one, rather laborious, method for calculating square roots in school. It was similar to long division but more complex. Newton's method, or various improvements on it, may be used. In the June 1981 issue of Byte Magazine, Stephen Wozniak shows how the value of 'e' (2.71828...) may be calculated to 116,000 places with an Apple computer. Unfortunately, it took about ten hours to make this calculation so a more practical approach is needed.

SYNPAD-A NEW CODE FOR ULTRA-HIGH SECURITY-Jack Schacter

Picking the Right Number

The two main criteria for selecting the irrational number are that the number must be calculable on a microcomputer in a reasonable time and that it be easily changed, when necessary, so as to assure security.

The first requirement is often met by numbers that can be calculated by using an infinite series expansion. Square roots, cube roots, etc., also trigonometric, logarithmic, exponential, hyperbolic, elliptic, Bessel, and many other functions are available. The series expansion of the selected number must be investigated in order to determine that it converges rapidly and that it does not require extensive calculations which would cause it to take an excessive amount of time to be performed on a microcomputer.

The second requirement may be fulfilled by using a transcendental function of one or more variables. For example, suppose the function R=Cos T were chosen. The value of R, the normal number, could be changed easily by using a different value for T, the Secret Key, whenever required. If required, the value of T could be changed for every message. This is easily accomplished by adding the date and time of each message to the Secret Key in order to form T. The computer would then calculate as many digits of R as may be required. The date and time of the message is sent in the clear preceding the encoded text so as to enable decoding. Every message thus has a different T and R.

The next step is to set up an algorithm to calculate Cos T to a large number of significant digits. This could be done by a straightforward programming procedure using the infinite series expansion of Cos T. Unfortunately, Cos T does not converge rapidly enough to be practical, so another function was used for Synpad.

The complete coding/decoding program then consists of three parts:

1. The first is an input section which requests the operator to say whether the message is to be coded or decoded, name the source message file and the output file, and to input the secret random number which will be used, together with the date and time, if desired, to calculate the Synpad irrational number. Of course, the Secret Key could be stored in the computer but then it is vulnerable to being stolen. Except for this key, revelation of the program does not compromise the coded messages.
2. The next section consists of the calculation of the Synpad normal number.
3. The last section encodes or decodes the source message and records the result under the name given to the output file.

A Practical Program

For Synpad, we have selected bei(T) to generate the normal number. bei(T) is a Bessel function which converges much faster than Cos (T) and can therefore be calculated much faster.

$$BEI(T) = \sum_{K=1}^{K=INF} (-1)^{(K+1)} \times \frac{T^{2(2K-1)}}{4[(2K-1)!]^2}$$

An examination of the function shows that the calculation may be simplified by noting the following:

1. The power of -1 simply changes the sign of each succeeding term starting with plus.
2. The constant "4" in the denominator does not increase the "randomness" of the function and so can be discarded.

The function to be calculated then becomes:

$$R = 4 \times BEI(T) = \sum_{K=1}^{K=INF.} (-1)^{(K+1)} \times \frac{T^{2(2K-1)}}{[(2K-1)!]^2}$$

SYNPAD-A NEW CODE FOR ULTRA-HIGH SECURITY-Jack Schacter

In order to reduce the time necessary to calculate R, a recursive method, which calculates each term from the last, is used. An algebraic calculation shows that the ratio of two consecutive terms is:

$$\frac{k\text{th term}}{(k-1)\text{th term}} = -1 \times \frac{T^4}{[(2k-2)(2k-1)]^2}$$

There are three parts to this expression. First, -1 indicates that the sign of consecutive terms changes. Second, the fourth power of T in the numerator shows that the value of each term rapidly decreases toward zero if T is less than one. Third, that the coefficient of T to the fourth power, the reciprocal of the square of (2k-2)(2k-1), is independent of T. Again, in order to save calculation time, this coefficient may be pre-calculated by another program and kept in disc memory as an auxiliary file.

Choosing the Input Number: " T "

Next, a method of choosing the input value, T, must be selected. The choice of T is intimately connected with the security that is required. If the computation algorithm should become exposed due to some failure in keeping the program or computer secure, then all that prevents decoding of the messages is determined by the value of T. If T has been randomized, then it can only be found by a trial and error process. With much fortitude, and enough money to pay for time on sufficiently fast computers, it will ultimately be found. Fortunately, however, encoded information has value only over a limited time period. Inside information which may affect the price of securities may be of value for only a few days. On the other hand, company trade secrets may have to be protected for years.

Calculating Degree of Security

Calculating the degree of protection is not very difficult. Let us suppose that the fastest computer extant can decode a message for a given value of T in one thousandth of a second and further that within the life of the encoded data, a computer which can accomplish this in one millionth of a second becomes available.

$$10^6 \text{ decodes/sec} \times 60\text{sec} \times 60\text{min} \times 24\text{hrs} \times 365.24\text{days}$$

$$= 3.16 \times 10^{13} \text{ decodes/year}$$

$$\text{10-byte hex number} = 256^{10} = 1.21 \times 10^{24}$$

$$\text{Average time to crack code (10-byte key)} = \frac{1.21 \times 10^{24}}{2 \times 3.16 \times 10^{13}} = 19.1 \text{ Billion Years}$$

* * * * *

No. of bytes in key	Average Time to Crack Code
1	128 microseconds
2	33 milliseconds
3	8.4 seconds
4	35.8 minutes
5	6.4 days
6	4.5 years
7	11.4 centuries
8	292 millennia
9	74.7 million years
10	19.1 billion years

Calculation of Synpad Security

Such a computer is far beyond of the present state of the art and it is extremely unlikely that this speed is attainable. Therefore, the use of this value is very conservative. The average time to break this code is given in the above table. The table shows that using six or more characters for T, the key number, results in a very long time, on the average, to break the code using the ultra-fast computer assumed here. If seven characters are used for T, the time is approximately 1140 years which should be long enough to discourage unauthorized solution.

In the event that you do not agree with the one-millionth of a second per decode as a potential capability, then substitute your estimate of computer speed and then calculate the number of characters that you will need in the value of T. The program can accept up to 144 characters for T. If this number of digits were used, the average time to break the code would be longer than the expected life of the universe, even if the decoding computer were billions of times faster than the one assumed above. Of course,the penalty for using that many digits in T will be a somewhat slower encoding and decoding time.

A Different Key Every Time

In order to prevent all messages from being encoded by the same random number, thereby easing the cryptanalysts' job of discovering it, the value of T may be changed for each message. This is usually necessary only for messages that must be sent by a common carrier system to which, it should be assumed, anyone has access. Otherwise, simply changing the key from time to time is adequate.

Using a different key for every message is accomplished by first selecting a Secret Key which will be the same for every message. To this number is added the date and time which will be different for each message. Of course, it would be wise to change the key at least once each year to reduce the possibility of discovery by unauthorized means or by chance.

While it is possible to calculate as many digits of bel(T) as we like, the time necessary to perform the calculation goes up as the square of the number of digits. Therefore, calculating 300 digits takes nine times as long as 100 digits. We can reduce the time by performing the 100 digit calculation, with a different T, three times. We accomplish this by dividing the message into "pages" of 128 characters.

Messages are then coded by page so that each page has its own value of T. This may be accomplished by adding a digit to the key number which is automatically incremented at each new page during both coding and decoding.

Calculating the Synpad Value "R"

Based on T and using the auxiliary file of coefficients, the value of R is calculated. The value of the first term, k=1, in the expansion of R is equal to T squared. After this initial value is calculated, all succeeding terms are calculated from the last as explained above. The calculation stops when the value of the calculated term is zero. Adding additional terms would clearly have no further effect on the value of R.

Each of these digits is then exclusively-orred with the ASCII value of each character in the source message. This technique is used, rather than adding the random number to the ASCII value, because it is faster and can be used for both coding and decoding.

Before encoding, an eighth bit is added to the ASCII value, if necessary, to obtain even parity. In decoding, if the decoded value of the character is not of even parity, we know that an error has occurred. This is indicated by recording the symbol "¶" instead of the character. Also, in order to increase the difficulty of decoding and to simplify recording on a floppy disc, all messages are made to be multiples of 128 characters. Dummy characters of odd parity are added to the message, if necessary, in order to fill out to an even multiple.

Long Messages

If the message is longer than 128 characters, then the page number is incremented, a new T and R are calculated and the next 128 characters are coded or decoded. This continues until all of the source file has been used.

Conclusion

Microcomputers provide a function here that mainframes do not duplicate. The very nature of a mainframe, its huge capacity and high hourly costs, necessitate that a large number of people have access. Almost always there is telephone access. Anyone who has had professional experience with computers knows that a determined person, who can get access to the computer, can also break into its files. The advantage of the microcomputer is that access is limited. The floppy disk with the program can be treated like cash by the very small number of people authorized to use it. The discs with clear data are treated the same way. The encoded data needs no security. Those disks can be stored anywhere, including the mainframe memory, and easily transmitted by modem or data lines.

Synpad is thus able to provide a data encoding system that can supply any degree of security that may be required and yet be easily and inexpensively handled on microcomputers. Synpad is published by **Family Ledgers Ltd.** of Bethpage N.Y.

****
Using The L.I.C.A. Bulletin Board System
Al Levy (Part 5)
****

Next keyword: (or press return to end HELP) PASSWORD
Help with protecting messages with password.

When you enter your message, you will be asked if you want to password protect it. If you say no, then anyone can kill it later (but presumably only the person you sent it to will). If you say yes, then you can either:

1. Enter a 4 character password OR
2. Press return to have the system protect the message.

In case 1, you, anyone knowing your password, or the system operators, will be able to kill your message. In case 2, only the system operators can kill it.

Next keyword: (or press return to end HELP) KILL
Help on killing (erasing) messages.

To kill (erase) a message, you use the "k" function. You'll be prompted for the message number. If the message is found and is killable, it's summary will be typed for verification that you entered the correct number. If it was saved with a password, you will be asked for the password.

Next keyword: (or press return to end HELP) K
KILL FUNCTION

To kill (erase) a message, you use the "k" function. You'll be prompted for the message number. If the message is found and is killable, it's summary will be typed for verification that you entered the correct number. If it was saved with a password, you will be asked for the password.

Next keyword: (or press return to end HELP) ERASE
Help on killing (erasing) messages.

To kill (erase) a message, you use the "k" function. You'll be prompted for the message number. If the message is found and is killable, it's summary will be typed for verification that you entered the correct number. If it was saved with a password, you will be asked for the password.

Next keyword: (or press return to end HELP) F
File downloading mode.

Next keyword: (or press return to end HELP) SUMMARY
Help with system summary function.

The (s)ummary function prints 2 lines for each message in the system, from a given starting message number. Use ctl-k to abort the summary listing. The summary prints:

MESSAGE NUMBER / NUMBER OF LINES IN MESSAGE / DATE CREATED / FROM / TO /SUBJECT

The (q)uick summary function prints only msg # and subject. You will be asked for the starting message number, (you need not enter leading zeros). Alternatively, you may enter a number of the form -n, where n is number representing 'the last n messages'. For example q;-15 would start the scan from the 15th most recent message. (Or, you could type q, then press return, and when asked for the starting message #, reply with -15). ";" is used to separate "anticipated" answers.

See help keyword "scan" for info on scanning messages for specific data (date, from, to, subject).

Using The L.I.C.A. Bulletin Board System
Al Levy (Part 5)

****

Next keyword: (or press return to end HELP) ? S
SUMMARY COMMAND

The (s)ummary function prints 2 lines for each message in the system, from a given starting message number. Use ctl-k to abort the summary listing. The summary prints:

MESSAGE NUMBER / NUMBER OF LINES IN MESSAGE /DATE CREATED /FROM / TO / SUBJECT

The **(q)uick summary function** prints only msg # and subject. You will be asked for the starting message number, (you need not enter leading zeros). Alternatively, you may enter a number of the form -n, where n is number representing 'the last n messages'. For example q;-15 would start the scan from the 15th most recent message. (or, you could type q, then press return, and when asked for the starting message #, reply with -15). ";" is used to separate "anticipated" answers.

See help keyword "scan" for info on scanning messages for specific data (date, from, to, subject).

Next keyword: (or press return to end HELP) ? SUMMARY
SUMMARY COMMAND

The (s)ummary function prints 2 lines for each message in The system, from a given starting message number. Use ctl-k to abort the summary listing. The summary prints:

MESSAGE NUMBER / NUMBER OF LINES IN MESSAGE / DATE CREATED / FROM / TO / SUBJECT

The **(q)uick summary function** prints only msg # and subject. You will be asked for the starting message number, (you need not enter leading zeros). Alternatively, you may enter a number of the form -n, where n is number representing 'the last n messages'. For example q;-15 would start the scan from the 15th most recent message. (or, you could type q, then press return, and when asked for the starting message #, reply with -15). ";" is used to separate "anticipated" answers.

See help keyword "scan" for info on scanning messages for specific data (date, from, to, subject).

Next keyword: (or press return to end HELP)? QUICK
HELP WITH SYSTEM SUMMARY FUNCTIONS.

The (s)ummary function prints 2 lines for each message in the system, from a given starting message number. Use ctl-k to abort the summary listing. The summary prints:

MESSAGE NUMBER / NUMBER OF LINES IN MESSAGE / DATE CREATED / FROM / TO / SUBJECT

The **(q)uick summary function** prints only msg # and subject. You will be asked for the starting message number, (you need not enter leading zeros). Alternatively, you may enter a number of the form -n, where n is number representing 'the last n messages'. For example q;-15 would start the scan from the 15th most recent message. (or, you could type q, then press return, and when asked for the starting message #, reply with -15). ";" is used to separate "anticipated" answers.

See help keyword "scan" for info on scanning messages for specific data (date, from, to, subject).

Next keyword: (or press return to end help)? Retrieve
Help with retrieving messages.

The retrieve ("R") function is used to retrieve a message from the system. You must know the message number, which you can find using the S (summary) or Q (quick summary) function. You will stay in "retrieve mode" until you press return to go back to the function menu. To retrieve multiple messages, use the format: R;1;12;347;486;123....;n when entering the retrieve mode, or just 1;12;456;763;122...;n when already in retrieve mode. It is not necessary to type the leading zeroes in a message number.

LOCAL NETWORKING - TOM GOLWAY

I) Background on Local Area Networks - Definitions

A LAN is a system of multiple interconnected devices that is:

1) privately owned, user administrated, not subjected to regulations by the FCC.
2) Structured in the sense that it is integrated into a discretephysical entity with all devices such as Word Processers, Facsimile, CRT's and CPU's are interconnected by a continuous structured medium.
3) Limited in geographic scope with devices physically seperate and non-mobile.
4) Supports any user to communicate to any other user.
5) High speed, generally greater than one megabaud.

BAND - is the frequency spectrum between two defined limits
BANDWIDTH - the difference between the limiting frequency of a continuous frequency band; in cycles per second (hertz)
BROADBAND - describes wide bandwidth, greater than voice grade channel (4KHz). Broadband equipment or systems carry a large proportion of the electromagnetic spectrum. Typical characteristics are high speeds with many channels.
VIRTUAL CIRCUIT - is the logical circuit established connecting an input port to an output port for the duration of the interaction between processes.
MESSAGE SWITCHING - is the absense of a circuit (both logical and physical), relying on destination addresses found in the messageitself so that the appropriate ports will receive the message.
NODE - is a single input/output device on the network, usually a workstation, but not necessarily.

LAN ATTRIBUTES

LAN's operate on data at high speeds over a geographically limited distance. To insure the integrety of the data, an error detection mechanism is included with a means of correcting the error. Usually this method of correcting an error is retransmission of the packet.

The data being transmitted is split in to groups called packets. Each packet has information pertaining to the source, destination and type of packet. In addition, there is additional information regarding other acknowledgements such as CRC, sequencing of packets, other types of addressing and various parameters about the protocol domain and character set.

Adding or deleting nodes to the network becomes a minor task because networks are fully distributed so there is no master list of nodes that must be defined prior to adding a node. This list is updated dynamically and the system continues to function. In reality, adding or deleting a node does cause momentary electrical noise on the cable, but with error detection and retransmission the network remains relatively unaffected.

II) Why LAN's Benefit

In the past, the computer industry grew up developing hardware and software to squeeze out every last ounce of efficiency from their large computer systems. In recent years, CPU cost/performance has improved dramatically due to revolutionary advances in silicon technology.

Now the cost of the CPU is no longer a major concern. Instead, the peripherals such as disks, printers, etc. sometimes cost more than the entire processor. Dedicated workstations are becoming the most cost effective way of providing a totally productive office environment. However, these systems are typically single user and there still exists the need for information interchange.

L O C A L N E T W O R K I N G - T O M G O L W A Y

Sharing of larger and more reliable peripherals is a must to achieve the concept of the integrated office. Large databases and high speed printers need to be shared and are to costly for a dedicated workstation to bear. A LAN provides such an environment allowing total resource sharing (other than CPU), file servers for large disk storage, print servers for high speed matrix and letter quality printers and high speed communication servers for links to wide area networks such as Telenet. LAN's allow for the total information interchange between normally incompatible nodes on the network. So there no longer is a need to rely on one single vendor for all devices. LAN's provide for higher speed and lower error rates then conventional point to point networks (RS232C). A LAN provides for total distributed intelligence so no dependence on any one node is necessary. If a node goes down, work still continues.

Typical applications:

Office Automation	Industrial Automation
- Electronic Mail and Memos	- Computer Aided Design/Manufacturing
- Word Processing	- Store and Forward Digitized Voice, Data, Fax, Mail
- Electronic Calendar	
- File and Records Management	

III) History

In the late 1960's the Department of Defense Advanced Research Projects developed a long distance packet switching network called ARPANET. This network originated the packet-switching protocol now used by many current LAN's. It lent support to the concept of interconnecting dissimilar computers for a loosely coupled CPU-CPU communications.

In 1972 Xerox Corp Palo Alto research center began work on what is now called Ethernet. Ethernet was announced in 1979 jointly with Digital Equipment Corp and Intel Corp. Currently over 30 companies are supporting Ethernet as the defacto standard.

Major contributions to the widespread usage of LAN's are

- Proliferation of microcomputers and some way of interconnecting them.
- Declining costs
- Adaptation of high speed mechanisms - coax cable, fiber optics.
- Growth of the office automation market.

IV) The ISO Seven Layer Reference Model

The International Standards Organization has produced a seven layer architecture for computer networks called the Open Systems Interconnection.

On each level of the reference model, a given node communicates with another node. All communication is supposed to remain at a particular level at all times. Rules and conventions used at this level constitute the protocol of the level. Since all levels are involved in every message, communication at a particular level is virtual. Actual communication occurs only at level 1 and is managed by link-level protocols at level 2, which serves the upper levels. Levels are joined by interfaces, each defines how the lower level serves the upper level.

The ISO model consists of seven protocol layers

1) Physical

The physical layer is concerned with the electrical and mechanical specifications, ie. signal levels and connectors. The function performed by the physical layer is the transmission and reception of an unstructured stream of bits over the network media. Protocols at this level involve such parameters as the signal voltage swing and bit duration, whether transmission is simplex, half or full duplex and how the connections are established at each end. Examples of standard level 1 protocols are RS232C, RS449, etc

2) Link

The link layer is concerned with the transmission and reception of a structured stream of bits over the network. The link layer provides the ability to take the unstructured bit stream from level 1 and sub-divide it into structured blocks of information. Acknowledgements, if any, are awaited for following each packet sent out. Link level protocols usually include a destination address, sometimes a source address and some means of error checking, many times a checksum at the end of the packet. Examples of level 2 protocols are HDLC, SDLC and CSMA/CD

3) Network
The function of the network layer is to facilitate the transmission and reception of a packet from a source node to a destination node within the network. In traditional point to point store and forward networks, packets are typically passed from source to destination through a series of intermediate nodes, and hence some algorithm for routing a packet to its final destination must exist. This is implemented in the network layer. Examples of protocols are X.25 an the interface message processors of ARPANET, which is also used on GE's Telenet.

4) Transport
The function of this layer is provide for reliable end to end communication over the network. Two basic strategies have evolved to support this, virtual circuits and datagrams.

Datagrams are self-contained messages which include source and destination addressing information and are delivered under the control of the transport layer protocols. Virtual circuit allow for logical point to point connections to be established between source and destination and provide for a reliable data stream to be passed over the circuit from end to end. Virtual circuit based transport services have been the most widely used to date.

5) Session
This layer takes care of the management of end to end communication between processes running on the network hosts. Typically the session layer provides facilities to map logical names into network address information meaningful to the transport layer. It manages interprocess communication within the network by opening, closing and sending data over transport layer virtual circuits or by sending datagrams, or both.

For example, in a database management system a failure of a transmitting node in the middle of a transaction will leave the database in an inconsistent state. The session layer organizes message transmissions in such a way that as to minimize the probability of such an error occurring.

6) Presentation
The function of the presentation layer is the transformation of data to be sent to or received from the network. For example to limit the amount of data being sent across the network, a data compression algorithm may be used. Data would be compressed in the presentation layer, sent out to the destination and then expanded again in the presentation layer. Similarly, data encryption algorthims would also be implemented in the presentation layer.

7) Application
The application layer is the one seen by the end user. At this layer, network transparancy is maintained, hiding the physical distribution of resources from the user and providing access to file servers, print servers, etc. that seem to the user, to be concentrated in their own workstation.

V) Topology
Topology is basically the pattern formed by the nodes on the network. Unlike long haul networks, LAN's stipulate a specific topology with which they are designed to work. Most LAN's use a broadcast topology, one which multi-addressing is employed. All messages are physically transmitted to every node, but a node only acts on messages addressed to itself. The most common types are bus, tree, ring and star.

Bus consists of a linear length of cable to which nodes are connected to by Taps (interfaces).

Tree is a variation of the bus. Tree topology splits the basic cable into smaller independent subsections which communicate with each other via a bridge at these junctions. Throughput in token bus networks decrease with each node added, and in contention networks, throughput is best in light bursty traffic and decreases in steady traffic environments. Failure of one station will not affect the rest of the network and a break in the cable will only affect part of the network.

Ring is a continuous loop of regenerative signal repeaters with cable links connecting each pair of repeaters daisy chained. Messages are relayed around the loop from one repeater to the next. Throughput decreases with each added node, and the delay is a fixed function of time depended on the number of nodes in the network. If one station fails, the whole network fails, unless bypass circuitry has been implemented in each interface or node. Unless the network design is relatively sophisticated, ring topology has the potential to be very unreliable.

Star is basically similiar to a multiuser computer system, but instead of terminals connected to a central system, there are intelligent workstations. Basically all depends on the central node. Throughput of the network is directly proportional to the internal bus capacity of the central node. If any node fails, the network continues to operate, unless it is the central node, in which case, the network fails.

VI) Access Methods

Access methods basically are a set of algorithms by which a user obtains access to a data channel on the network. The two main types are Carrier Sense Multiple Access with Collision Detect (CSMA/CD) and token passing.

CSMA/CD is basically a listen, then send technique. Only one node may transmit on the bus at any given time, so the node first listens to the channel to hear is any other node is transmitting. If the channel is busy, the node waits until the channel is idle. When the channel is idle, the node then transmits a packet. If two nodes originate a transmission at the same time, a collision occurs, destroying the integrety of the packet. The node detects this collision, waits a random amount of time before trying again. CSMA/CD is best suited to networks which have intermittent traffic in which throughput and low delay are more important than guaranteed access. It works well as long as the traffic remains medium to low. As the traffic increased, so do the chances of collisions and cable busy's. Xerox conducted bechmark tests which showed that under normal load conditions, collisions are rare.

Token passing networks are essentially a series of point to point cables between consecutive stations, each of which actively participates in the control of the network. One or more tokens made up of a special unique bit pattern travel around the network when all nodes are idle. When a node wants to transmit a packet, it must first seize control of the token and remove it from the network. This is accomplished by transforming the token into a connector pattern of bits. The node is then free to transmit and the other nodes remain idle. When finished, the node transforms the token into it's original state and sends it back on the network. Token passing is best suited to networks with a few very high speed nodes that are in close proximity to one another and require guaranteed access to the network. For example a real-time process control application.

VII) Medium

Current LAN media technology consists of twisted pair wire, baseband coax, broadband coax, and in the near future, fiber optics.

Twisted pair wire supports all topologies with a maximum distance of about 25KM. It is a single unidirectional channel with the capability of either analog or digital signals depending upon the modulation, and can be either half or full duplex. The maximum bandwidth is generally up to 10M baud. The major advantage it has is its low cost. It has high error rates at high speeds because of its low immunity to noise and cross talk.

Baseband LAN's typically use a bidirectional signal path on which signals are encoded onto the cable using some baseband method such as Manchester encoding. An example of this is Xerox Corp. Ethernet. Since all data is carried on a single channel in baseband, it needs a high data rate and short packet size. Short packets demand a short propagation delay to maintain superior performance. Hence, baseband LAN's such as Ethernet limit the total propagation delay leading to a limited distance of 1-3KM. Baseband LAN's use a passive medium with digital techniques based on voltage differences used to transmit data. The maximum bandwidth is up to 10Mbaud and can support up to 1024 nodes. Baseband coax lacks the physical ruggedness needed in hostile environments and the bandwidth can only carry about 40 percent of the load to remain stable.

Broadband coax has some major advantages over twisted pair and baseband coax. This method uses standard cable TV media technology which can support an aggregate total bandwidth of 400 MHz. By using frequency division multiplexing, broadband can support several channels. A large diversity of communications equipment is available in the 300-400 MHz spectrum so an office can be totally integrated with all information flow on one cable pathway. This means that voice, data or video signals can operate on the same cable thus reducing installation costs significantly.

Broadband coax is an active medium. It requires power to drive the network which is based in the networ components rather than in the user workstations. Signals are transmitted on the cable using F modulation techniques, using a RF modem. Broadband is half duplex so there needs to be seperate transmi and receive lines. This can be accomplished by either splitting the 300MHz bandwidth into send ar receive channels or by using seperate cables. By using active amplifiers to distribute and exten signaling range, broadband networks retain full bandwidth over large distances. It has better immuity t noise and interference than baseband, and is rugged and durable. It also can tolerate 100 percent of th bandwidth with off the shelf products.

Fiber Optics is the real threat to coax based LAN marketplace. Fiber optic cable consists of a thi central core of glass or plastic that has a high index of refraction. This fiber is surrounded by cladding layer that has a slightly lower index and isolates its central fiber from the several othe fibers in the cable. Each fiber provides a single unidirectional point to point transmission path. single-encoded lightbeam is introduced onto the fiber by a laser or LED, and is transmitted along th fiber by reflection against the core. Current bandwidths are limited to the 50Mbaud range for network with a geographic scope of up to 10KM. Multipoint broadcasts, bandwidth up to 400Mbaud, multipoin connections and multiplexing of light frequencies using the color spectrum have been demonstrated in th laboratory environment.

Fiber optic transmission is unaffected by electrical interference, noise, crosstalk, power outages an even tolerant of adverse temperatures, chemicals and radiation. Any type of signal can be encoded voice, video or data. Physically, the cable is small, light weight, able to fit into limited duct space and highly secure since it is difficult to tap.

In summary, a LAN provides for total distributed intelligence so no dependence on any one node i necessary. If a node goes down, work still continues. Tom Golway

A Byte to the Core - Erik Klein

This has most certainly been an interesting month for me as far as cleanliness goes! My system seems to think that it is Christmas (Chanuka) for all the gift it got. (When you are into computers all you can afford is one.) I also would like to share a secret and give a recommendation in this column.

First the secret. There is a disk drive that is better than the one IBM will most probably sell you! True, IBM does use the company that makes these drives as a second source, but I have yet to see one of these drives with an IBM serial number. The manufacturor is Control Data Corp. and the drive is noiseless. Noiseless is not the product name but an adjective that I feel describes these drives beautifully. Not only are they quiet but they sell for about half the price of one IBM drive. As a matter of fact you can acquire two boxes of disks as well as a pair of these beauties for about the same price as one IBM label drive, and they are better pieces of equipment! In the three weeks that I have owned them I have used them more then I will in the next three months, but they have stood up beautifully! But enough about disk drives I have more to tell you.

Have you ever realized that your PC probably gets bored when it is not in use? Don't feel bad if you didn't because I didn't either. This ignorance on my part was rectified immediately when I opened my system unit and removed my single sided disk drives (boat anchors). I know now what I didn't know before the removal of the drives. As it turns out my computer was bored; bored enough to start a collection! Now you must realize that a computer does not have a mind like you and I do, it thinks on an entirely different wavelength. Where a protoplasmic being collects coins or stamps, the silicon mind goes for dust! Not only that, the computer, being an impressively efficient mechanism, is a marvelously efficient collector! When I went to remove my drives I was almost crushed under an avalanche of dust! The suction that is caused by the fan draws the dust in under the disk drives and traps it there. This dust also spreads out so that it covers your system board and your power supply causing potential heat problems (especially with new mother boards). Fortunately there is a remedy for this! Clean your system unit! This is no simple task but it is do-able.

The first thing that you will obviously have to do is remove the cover from your system unit. If you do not already know how to do this check your guide to operations. After you have the system unit cover off check some of the chips on your option boards and on the disk drives. If they are fairly clean then replace the cover; your system does not really need cleaning. If they are dusty you can brush them off gently with a clean dry, static free rag or cloth. MAKE SURE THAT YOU DO NOT RUB OR BEND THE CHIPS AND OTHER COMPONENTS! After carefully cleaning the dust from your boards (don't forget mom) you can remove the drives. (If you can't check the Guide to Operations manual again under drive installation, do it backwards). Clean the plates under the drives and under the plates themselves by pulling your rag across or under them. After this make like the wind and blow, either with a vacuum cleaner or your lungs. Do not inhale during this step! If you are using a vacuum (make sure you use the blower nozzle) do not touch the system board or any component with the nozzle. Blow off the power supply and the fan then blow the disk drives clean in the same way. When you think you have the system clean replace the components and the drives. The outside of the unit and the keyboard case can be cleaned with a lightly soaped sponge and the keys can be individually cleaned with the same items. Be sure to remove the keys before cleaning them so that you do not destroy the keyboard electronics. Be just as careful with the system unit. Good luck and happy cleaning! Erik Klein

****

I M P O R T A N T   N O T I C E !

Please help. Doug McGarrett needs a SIGNETICS 8T16 IC immediately if not sooner.

If you can help to locate this chip call:

(212) 464-4487

****

The Long Island Computer Association, INC. is open to everyone, amateur or professional with an interest in computers, computer applications, programming, or related subjects. Dues are $12.00 per year which includes monthly issues of this publication. The STACK is mailed to other computer clubs on an exchange basis as well as to various technical publishers. Permission for reprinting or quoting items in The STACK is granted providing that credit is given & a copy of the reprint is sent to The STACK. Members can vote in club elections, & place non-commercial classified ads(at no charge) and commercial ads at nominal cost. Member articles and other data affecting The STACK must be received by the 15th day of any month, to be published in the following issue. All copy should be sent to: Al Levy P.O.Box 71 Hicksville N.Y. 11802 (516) 293-8368

APPLICATION FOR MEMBERSHIP (Please Print)

Name: ______________________________

Address: ______________________________

City/State: ______________________ Zip: __________

Telephone: ______________________ Date: __________

Computer Equipment Owned:(OPTIONAL)

____

____

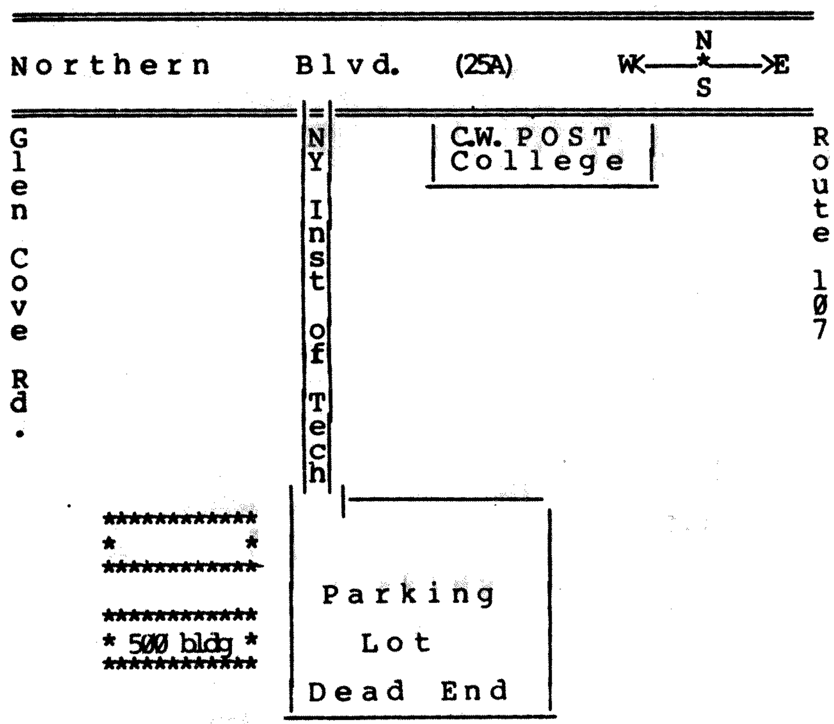
Reccomended to LICA by: ______________________________

Please enclose $12.00 DUES and send to:

L.I.C.A. P.O.BOX 71 HICKSVILLE,N.Y. 11802

* If your are applying after July dues are $6.00 until January

The Stack LONG ISLAND COMPUTER ASSOCIATION
PO BOX 71 - HICKSVILLE, NY 11802



PLEASE RUSH TO:

BULK RATE
U.S. POSTAGE
PAID
PERMIT 44
JERICHO, N.Y.

ADDRESS CORRECTION REQUESTED