

University of Alabama in Huntsville

LOUIS

Office of Information Technology (OIT)

Historic University Publications

1-1-1993

Office of Computer Services Magazine 1993

University of Alabama in Huntsville

Follow this and additional works at: <https://louis.uah.edu/oit>

Recommended Citation

University of Alabama in Huntsville, "Office of Computer Services Magazine 1993" (1993). *Office of Information Technology (OIT)*. 2.
<https://louis.uah.edu/oit/2>

This Newsletter is brought to you for free and open access by the Historic University Publications at LOUIS. It has been accepted for inclusion in Office of Information Technology (OIT) by an authorized administrator of LOUIS.

@UAH.EDU

Volume 2, Number 1 Computer Services Magazine Spring/Summer 1993

Contents

Laserjet Printing	1
Speed Typing	1
Hands in the Cookie Jar	3
User Request Automation	4
Acquiring Information from A. A.	5
Microsoft Excel Macros	5
SYSTAT Licenses	5
ASN Solicitation for Professional Services	6
Using the ASN Mass Storage System	7
What is Administrative Applications?	15
Downloading Class Rolls	16
Mother Says	17
Campus Computer Security Policy	19
Is your PC Cable Ready?	26
DEC CampusWide Software License Grant	27
Software Piracy	27
UAH Computer Labs	30
UNISYS Computing facilities	32
CS Software Support Policy	33
Network Address Form Instructions	34
Network Address Form	35

New Hardware, Software For The University

By Mike Meyer
Director, Computer Services

The University has only about 32 months left on the current lease with Unisys corporation. With that in mind and the recommendations of the 1990 MIS study the Computer Center has been looking at alternative computing resources. The most attractive combination of software and hardware are a DEC 7000/610 and SCT administrative software.

The 7000/610 would be a unit processor running at 182 Mhertz, 128 Mbytes of memory and 16 Gbytes of DASD. In addition we would have a 2000 lpm printer and two tape drives - each capable of backing up 42 Gbytes of disc unattended. These drives were chosen so that sometime in the future the Computer Center could back up departmental servers on the campus network.

The SCT software would include integrated packages for Accounting (FRS), Accounts Payable & Purchasing (FPR), Bid module (BID), Inventory (FXX), Budget development (BDS) and Human resources (HRS). Information Builder's FOCUS would be used as a report generator for the above systems. Also included in the proposal is the VISAGE software product. This product enables users of the SCT products to use the software in a Windows GUI(Graphical User Interface).

This configuration is highly attractive from several perspectives. The SCT administrative software would simply be an upgrade to what we are currently running. This is nice from the learning/teaching aspect. The operating system and a large library of software is already licensed to the University for this machine in the form of the DEC CSLG/ESL. Also attractive is the fact that our researchers would have a code compatible machine on which to run overflow work from their departmental processors. ■

Directory

Computer Services 895-6347

	Ext.
Computer Room	233
General Delivery Mailbox	100
PC Trouble Mailbox	270
Meyer, Mike (Director)	223
Moore, Darlene	222
Wiley, Sandra	221

Administrative Applications:

Baxter, Felix	225
Braudaway, Michael	247
Demirjian, Ginger	227
Dossey, Eric	226
Greenwood, Jean	229
Kennedy, Jeanne	234
McComb, Laura	236
McCormick, Shirley	237
Perkins, Mary	240
Pringle, Miranda	241
Rice, Malcolm	242
Stanton, John	261
Tanev, Wayne	244

Network Services:

	Ext.
Albright, Chris	224
Gossett, Frank	228
Hall, Carey	230
Hampel, Larry	251
Hemphill, Rich	231
Humphrey, Earl	232
Looger, Joyce	235
Morphew, Larry	239
Mullican, Joe	277

Systems:

Allbritton, Bill	276
Lovell, Sandra	271
McCullars, Jim	238
Merrell, Becky	272
Moore, Randi	273
Sweeney, Barbara	243
White, Paula	274
Woodard, Jerry	275
Youngblood, Paul	245

Fax Machine 895-6643

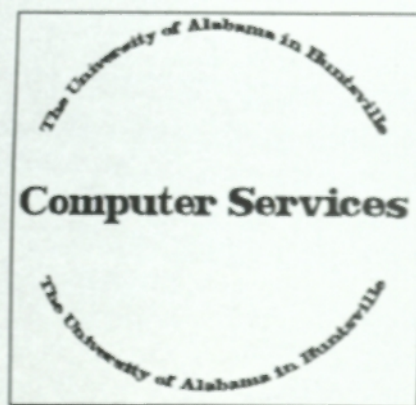
@UAH.EDU

Editor:

Michael J. Braudaway

Published Semi-Annually in September and March by the Computer Services Department of the University of Alabama in Huntsville. The opinions expressed herein are not necessarily those of the management of Computer Services. Subscriptions are available at no cost to any individual or organization. To obtain a subscription, complete and return the form on the back cover. Portions of this publication may be reproduced or reprinted for any non-profit purpose with an appropriate credit line. Send correspondence to:

University of Alabama in Huntsville
RI Annex B
Huntsville, AL 35899
Attn: @UAH.EDU Editor



The University of Alabama in Huntsville is an equal opportunity institution and welcomes applications for employment and educational programs from any individual regardless of race, color, sex, age, national origin, handicap, or veteran status.

LaserJet Printing

by Michael J. Braudaway

In a quest to do away with special forms, Administrative Applications has redesigned some of the many forms on campus for use on laser printers.

The new forms replace those formerly printed on the Computer rooms' impact printers. The forms, designed using the HP PCL 5 language, can be printed on demand in the office or transferred to Printing Services for printing large batches.

With laser printer forms there is no need for a special forms request in the computer room that requires an operator to mount special forms and then burst them. This saves the department the expense of setting up and stocking the special forms and saves Computer Services the labor of printing and bursting them. Some of the forms designed include Student billings, Labor Distribution and Bid forms.

While most small jobs are printed in the office, large orders are usually transferred to Printing Services for completion. The recent connection of the Printing Services building to the campus network has aided in the transfer of large files to the high-speed printer, the Xerox DocuTech. Jobs such as the mass printing of student bills and grades (tasks that formerly took hours to print) are now sent to PS to be printed using the DocuTech. ■

Speed Typing

by Carey Hall

When I first started working for UAH I was a computer operator. I loaded programs into the computer with a card reader. I loaded tapes on tape drives and pulled printouts off the printers. Other than pushing a few buttons now and then that was about it. Then the university made some kind of deal with Sperry to buy a new mainframe and, for the deal, Sperry would sell UAH a bunch of personal computers at a really good price. UAH went for it and really loaded up on these Sperry computers.

Dr. Jafar Hoomoni headed up the deal with lots of funds through project ACCESS. Wayne Tanev was my supervisor at that time and he was also involved with the computer deal. Sort of working for Dr. Homoni in addition to the systems manager for Computer Services. They even took Earl Humphrey away from the Physical Plant to help with the process. Well, they passed out PCs to just about anybody that showed any interest and to some that were not interested at all. I guess on the average it would be anywhere from 10 to 15 a day. One even ended up in the computer room and that's where I got to learn a little about them.

The deal with Sperry was that they would also maintain the PCs, for a small fee of course. Wayne and Earl would assemble the PCs and deliver them to the different departments around campus, then pick them back up if anything went wrong with them and have Sperry work on them. If you worked for UAH and wanted a personal computer for your very own you could buy one at a

special price. I remember a Sperry PC with a color monitor, one 360k floppy drive ,a 10 meg hard drive and 256k of ram was only \$5500.00. What a deal. Some went for it.

Anyway, Wayne became the Mapper guy and I became the operations supervisor and the guy dealing with all the PCs. Now we get to what this is all about. Whew!!!

When it all started computers were used mostly for word processing and games. There seemed to be a lot more games than word processors, too. My dealing with computers was mostly from the hardware aspect. Upgrading the memory and what not. I knew very little about any of the software. As I got more into it I found that most problems with computers had nothing to do with the hardware but the software running on them. Then there was always the O.H.G. you had to look out for. That's short for operator head gap.

I learned about all that was needed to deal with the software. You could make a bootable disk and load Wordstar on it and you could type your letter save it on B: drive and/or print it on your printer. **You had a nice letter or memo ready to go.** Remember, these machines had no hard drive and only 256k of memory. It didn't matter how fast you typed, the computer could keep up. If you wanted to check your spelling you could, simply by putting in a different diskette. The floppy drives were only 360k drives too. Then, the first thing you know there are other word processors around and even some newer versions of Wordstar. Well, these new word processors could not run on those old machines. Now you had to have a 10meg hard drive and 640k of memory. Oh boy, could those suckers hum. Now you had no chance of out-running it from the keyboard. It could process those words faster than you could think them, let alone type them in. Now days it seems, if you don't have at least a 486 CPU, 200meg hard drive, and at least 8meg of ram, you haven't got enough computer to do anything. So you take these new big, fast computers and you type real fast trying to make that computer really hum. Guess what you get? **You get a nice letter or memo ready to go.** What's the deal? Where's it all going? How much horsepower does it take to write a simple letter or a really complex one for that matter?

Well, I'd better close for now, I think my 486 Mhz CPU, my 200 meg hard drive, and my 8 meg of ram is starting to heat up. Plus I think my keyboard is starting to melt.

Next time. A walk through a Windows wonderland. ■

Hands in the Cookie Jar

by Chris Albright

When someone gets caught breaking into a computer, who is to blame? Is it the dastardly spy type who uses nifty electronic gear to hack into the system for secrets, or is it the haphazard system administrator who through no fault of his own has left the open cookie jar too near the edge of the counter? Or is it the programmer who writes his account password on a pad next to the computer. Maybe it is the operator who uses as a password operator to log into the operator account. These shortcomings in security may not be too severe where there is one computer. Then, enter the network.

Networks allow 24 hour access to most midsize computing systems. Because of the research and processing needed today, computers sometimes never turn off. Even when we are safe asleep in our homes, computers and networks are humming away. No more cold war, no more worry you say? What about that crystal thingamabob that does it on earth and not in space thingy you invented on a \$12,000 grant. That could be someone else's bread and butter if got to industry before you got that patent. From accounts in the media, European and Japanese firms employ industrial spies for just such purposes and have for some time.

If all this has made you paranoid, good. You should be. You may say: "we don't have anything anyone would want." That may be true, but it takes time to find, debug, and fix a problem someone caused by just looking. Weeks of work can be lost if there is no regular backup of systems. There are things we can do, simple things like passwords, that can deter this from happening. Some are:

- Thy password must be sacred and monogamous (Don't give it to anyone.).
- Thy password shall be difficult to guess (Don't make it your spouses name.).
- Thy password shall never be inscribed (Don't write it down.).
- Thy password must change often (Every 30-60 days is good.).
- Thy password must be new and clever each time (JIGMAFU anyone?).

Computer Services has worked long and hard on a security manual for computing at UAH. It would be well worth the time to take a look at it. There are some good guidelines to follow. It may be true that we are not building atomic bombs at UAH, but the information is important if only for the labor dollars spent on it. Don't give it away or make it easy to access.

Sometimes it may be true that we leave the cookie jar too close to the edge of the counter, but don't forget that sometimes the cookie jar might just fall off on the head of the child who steals. ■

User Request Automation

by Malcolm R. Rice

The process of submitting information requests and programming changes to Administrative Applications will soon become automated. This automation will be accomplished through the

Spring/Summer 1993 @UAH.EDU 3

implementation of the On-line User Request System (OURS), currently in the testing phase. OURS is an automated request entry and tracking system that will aid the user in submitting requests to Administrative Applications.

OURS utilizes COBOL-embedded SQL make calls to an RDB database located on a VAX. Users within the university community will be able to logon to the system either through ethernet connections or dial-up using a modem.

With the full implementation of OURS, the proper completion, including documentation, of programming changes can be monitored. Eliminating the unnecessary paper flow and ensuring that the proper person(s) authorize the request are two additional benefits derived through the use of OURS. Users will be able to enter request ideas and, at their convenience, submit them to Administrative Applications for disposition. Once a request is entered into OURS, it will be assigned a request number that is used to track the request. Through the use of request status codes, users will be able to determine exactly where the request is in the system.

System Users

Users of the system have been divided into four main types. The *Contact* is the person initiating the request. The *Administrative Authority* is the person who is responsible for committing departmental resources to fulfill the request. The *Information Security Coordinator (ISC)* is located within Administrative Applications. This person is charged with the duty of assigning the request to the programmer and monitoring the completion of that request. The *Programmer* is the person responsible for implementing the request to the users' satisfaction.

Request Status Codes

The system assigns status codes to the request being entered. A code of 10 indicates the request has been entered by the contact. No action is taken on these requests by Administrative Applications. A code of 20 indicates to the system that the request has been submitted by the contact to the Administrative Authority for approval. Requests with the status code of 20 and the Administrative Authority's "signature" are submitted to the ISC. A status code of 30 indicates that the request has been assigned to a programmer. Requests completed by the programmer have a status code of 50.

Users of the system will be able to view requests from their point of contact forward. Requests can only be modified before they move to the next level of approval. For example, a contact will no longer be able to modify a request once the status has been changed to a status 20, submitted to Approval Authority.

System Security

In addition to the request status codes each user, based on their function as described above, will be assigned a security code by the ISC. This code will indicate to the system the status of the user and the level of authority they have within the system. Contacts are assigned a security code of 10. The Administrative Authority is assigned a code of 20. The ISC has a code of 30. Active programmers have a code of 40.

System Views

Menu options, Reports, and Request Status access will be restricted by the security level of the individual. Contacts will have a different system view from the Administrative Authority, ISC and Programmer. Complete details of the system and its functions will be provided in the On-line User Request System User Documentation that will be available once the system goes into full release. ■

Acquiring Information from Administrative Applications

Every group/department on campus at sometime requires a subset of data on students, faculty and/or staff. There is a procedure for acquiring this subset which is mandatory for timely resolution of the request. The "owner" of the data must issue the request to Computer Services. Administrative Applications personnel can extract subsets of data only through the behest of the "owner" of that data. Therefore, if a department wishes information on a student population, the department must make the request through the Admissions or Records office. If a department wishes information on staff/faculty, the department must make the request through the Personnel office. ■

Microsoft Excel Macros

Microsoft Excel macros are currently being used to simplify daily activities of the university's accounting department. These macros replace manual procedures, such as rekeying of information, and allow workers more time to complete other tasks.

Computer Services has written macros that take downloaded text files from the mainframe and load the information into user's spreadsheets. This was previously keyed in by hand from departmental budget statements. These macros allow the department to increase the accuracy and productivity of its workforce.

Computer Services is trying to automate (where possible) spreadsheet tasks that can be simplified by macros. If your department uses Excel and has a routine job that crunches numbers in a spreadsheet, Microsoft Excel macros may be the answer. These services are available by contacting *Felix Baxter* at (205) 895-6347 ext. 225. ■

SYSTAT Available for WINDOWS and MACINTOSH

We have recently updated the campus site license for the SYSTAT statistics package to include the Macintosh and Windows versions in addition to SYSTAT for MS-DOS and for Networks which were previously available. SYSTAT is a very powerful statistics package which includes many statistics and graphics options. A demo disk is available for SYSTAT for the Macintosh

and SYSTAT for DOS but none is available for SYSTAT for Windows. All versions include the graphics options of SYGRAPH.

To obtain a copy of SYSTAT for Windows bring two formatted high density floppy diskettes to room M-30 or room M-1A of the Research Institute. For the Macintosh version, bring three diskettes and the model of the Macintosh. Installation instructions will be provided; however, users desiring full sets of documentation will need to purchase them. The cost of the Systat site license varies with the number of users, so if you are currently not using a copy you previously obtained, contact Computer Services so that we might update our records to reflect this.

Other site licenses available at UAH are as follows:

<u>Product</u>	<u>Functionality</u>	<u>Operating System</u>
ESL	Library of software	VMS
Procomm Plus	Asynchronous communication	MS-DOS
Janus/ADA	Language compiler	MS-DOS
MBP Cobol	Cobol compiler	MS-DOS
EZ	Text editor	MS-DOS
Novell	Local area network	MS-DOS
NCAR	Graphics library	Unix and VMS

Alabama Supercomputer Network Solicitation for Professional Services

The Alabama Supercomputer Authority (ASA) has requested proposals for operation and enhancement of the Alabama Supercomputer Network beginning in October 1993. The ASA released a Solicitation for Professional Services (SPS) in late October, 1992 and is now evaluating proposals submitted by vendors. Currently, the ASN is operated by Boeing Computer Services under contract to the ASA.

The SPS requirements include, briefly:

- Facilities management services for the ASN and the computer facilities of the George C. Wallace Supercomputer Center in Huntsville.
- Applications Analyst services at the 6 research universities in Alabama.
- Enhanced supercomputing services to replace the ASN CRAY X-MP with a supercomputer at least three times faster.
- Telecommunications services for the network communications circuits and ASN equipment.
- Visualization services for the Supercomputer Center and the research universities.
- Additional equipment.

The intent is to award a contract to a single vendor, with either a 3-year or a 6-year term. The ASA is currently evaluating proposals received from three vendors - Boeing, Nichols Research Corp. and EDS, Inc. An announcement of the chosen vendor and the term of the contract is expected at the end of March.

Using the ASN Mass Storage System

1. Introduction

The ASN acquired the UniTree Mass Storage System (MSS) in the summer of 1992 for four major purposes:

- to significantly increase user file space.
- to reallocate CRAY and Sun disk, in order to provide better service on these machines.
- to provide users a single file structure on both the CRAY and the Sun/nCUBE, using NFS (Network File System).
- to provide automatic migration of unused files to tape.

The CRAY and Sun disk previously used to store user files has been reallocated to the system on these machines. Several benefits result. Both machines have increased `/tmp` space. On the CRAY, more swap space is available, so more large memory jobs can be run and the full 16 million words of CRAY memory can be used.

The Network File System (NFS) is a service that enables machines to share files across a network. NFS permits transparent access to remote file systems, as if they were local to the user's machine. To the user, all files accessed through NFS look just like local files. With the MSS and NFS access to it from either the CRAY or the Sun, you do not have to keep duplicate copies of files on both machines.

There is a modest price to pay for NFS file access; it will always be slower than file access from a local file system, such as `/tmp`. In most instances, you will not notice this difference. However, if you are doing I/O intensive work on the CRAY, the slow access speed of the MSS will deteriorate your computing performance. See Section 7.

2. The MSS Hardware

An IBM RS/6000 Model 530H workstation controls the UniTree hardware, which consists of a cache of 16 857-MegaByte disk drives (13.7 GigaBytes) and an autoloader tape robot.

The tape robot has two 5 GigaByte 8mm tapes drives and 54 slots to hold the 8mm tapes. Five tape slots in the robot are reserved for system maintenance; the remaining 49 tapes are available for user files. Each user file is always written to two different tapes, so that files can still be retrieved in the event of a damaged tape. Thus, the total tape capacity directly accessible by the robot is one-half of 49 times 5 GigaBytes, or 122.5 GigaBytes.

Figure 1 shows the connections between the Mass Storage System, the CRAY X-MP, the Sun/nCUBE, and the remainder of the ASN. The connections are made through Fiber Distributed Data Interface (FDDI) optical fiber.

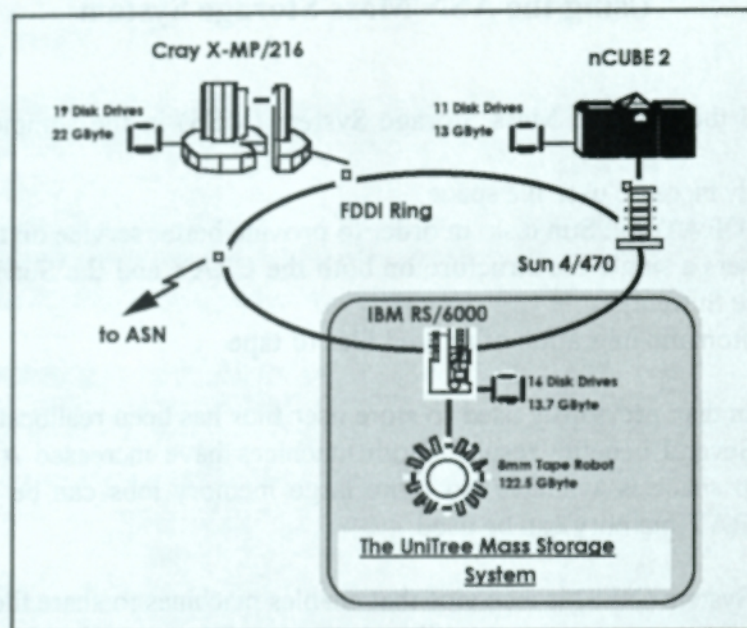


Figure 1

The UniTree Mass Storage System is available from all components of the Alabama Supercomputer Network

The tapes in the robot tape subsystem are not like other tapes which you have previously used, such as 9-track and cartridge tapes. You have no control over where your files are placed on the tape subsystem, and the tapes cannot be accessed directly by you, via tar or other UNIX tape utilities. You cannot have your own private tape in the MSS system.

While the total file capacity of the MSS is only limited by the number of 8mm tapes available at ASN, the on-line capacity is 13.7 GigaBytes of cached disk and 122.5 GigaBytes of robot-accessible tape. Any file in this space of 136.2 GigaBytes can be accessed without human intervention. The UniTree will issue a tape request for a shelved tape if a file is not on-line.

3. File Structure on the CRAY and Sun

Both the CRAY and the Sun access the MSS via the Network File System (NFS), so these machines view files on the MSS as part of their respective file systems. Files for both machines will be accessible by you from either machine, because both the CRAY and the Sun are NFS mounted to the same device. Figure 2 shows the file systems for both machines.

Despite the fact that you have access to all of your files from either machine, you must remember that binary files (such as executables and object files) made by one computer will be incomprehensible to another computer. For instance, you cannot expect the Sun or nCUBE loader to understand an object file that was created by the CRAY compiler.

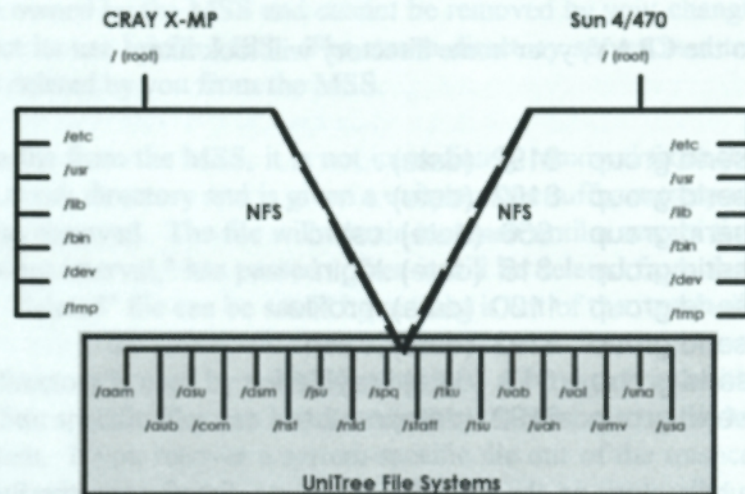


Figure 2
File systems on the CRAY and Sun

The UniTree and NFS collectively place the following limits on MSS files and file names:

- No file on the MSS can be larger than 2 GigaBytes.
- Device-specific files cannot be created on the MSS, via the **mknod(2)** command. For the general user, this means that named pipes (FIFOs) cannot be created on the MSS.

These limits may be further restricted by the computer you are working on.

The CRAY has a 14 character filename limit on its local disks. This limit does not apply to the UniTree -- you can create files with long names in the MSS. However, if you copy a long-name file from the MSS to a CRAY disk (such as /tmp) the filename will be truncated to 14 characters.

Both symbolic and hard links are supported on the MSS. Symbolic links are supported across file systems, so files on the MSS can be symbolically linked to a file in /tmp on the CRAY disk. Hard links are not supported across file systems. Hard links can be created between files on the MSS.

The home directories for the CRAY and the Sun will point to slightly different places in the MSS (Figure 3), in order to prevent the inadvertent mixing of system dependent files.

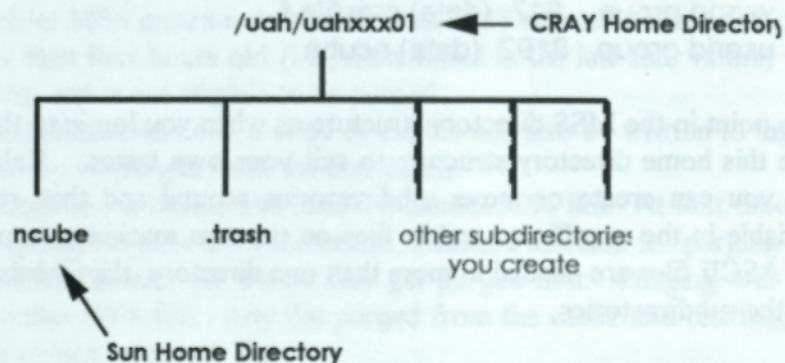


Figure 3
Locations of your home directories on the CRAY and Sun

When you log on to the CRAY, your home directory will look like:

```
asncray> ls -la
drwx----- 1 userid group 8192 (date) .
drwx----- 1 userid group 8192 (date) ..
-rw----- 1 userid group 656 (date) .cshrc
-rw----- 1 userid group 315 (date) .login
-rw----- 1 userid group 1130 (date) .profile
drwx----- 1 userid group 8192 (date) .trash
-rw----- 1 yserid group 617 (date) crayfile.f
drwx----- 1 userid group 8192 (date) ncube
```

where the **ncube** subdirectory on the CRAY is the home directory on the Sun. Similarly, when you log on to the Sun, your home directory will look like:

```
asncube> ls -la
drwx----- 1 userid group 8192 (date) .
drwx----- 1 userid group 8192 (date) ..
-rw----- 1 userid group 400 (date) .cshrc
-rw----- 1 userid group 413 (date) .login
-rw----- 1 userid group 898 (date) .profile
-rw----- 1 userid group 543 (date) sunfile.dat
```

You can move up one level from your Sun home directory:

```
asncube> cd ..
asncube> ls -la
drwx----- 1 userid group 8192 (date) .
drwx----- 1 userid group 8192 (date) ..
-rw----- 1 userid group 656 (date) .cshrc
-rw----- 1 userid group 315 (date) .login
-rw----- 1 userid group 1130 (date) .profile
drwx----- 1 userid group 8192 (date) .trash
-rw----- 1 yserid group 617 (date) crayfile.f
drwx----- 1 userid group 8192 (date) ncube
```

and see the same point in the MSS directory structure as when you log in to the CRAY. You are free to rearrange this home directory structure to suit your own tastes. Relative to the CRAY home directory, you can create or move subdirectories around and then redefine the HOME environment variable in the **.profile** or **.cshrc** files on the two machines to point to the desired subdirectory. If ASCII files are needed in more than one directory, then symbolic links to the file can be placed in the subdirectories.

4. The **.trash** Directory

The UniTree software provides a safety feature to protect you from accidental file deletions -- the **.trash** directory. This directory resides on the home directory of your CRAY account. The

.trash directory is owned by the MSS and cannot be removed by you; changing permissions on it also does not affect its use by the MSS. The **.trash** directory serves as a temporary holding bin for files which are deleted by you from the MSS.

When you delete a file from the MSS, it is not immediately removed from the system. Instead, it is moved into the **.trash** directory and is given a unique name suffix corresponding to the date and time at which it was removed. The file will remain in **.trash** until a certain time interval, known as the "trashcan time-out interval," has passed. Then it will be deleted from the system. Before this final deletion, any "deleted" file can be saved by moving it out of the **.trash** directory.

The same **.trash** directory is used by the MSS when you are logged onto either the CRAY or the Sun. CRAY and Sun specific files can be intermixed in the trashcan by the MSS when you delete files on either system. If you recover a system-specific file out of the trashcan, it is up to you to know which computer it came from.

The default time-out interval is 10 minutes, but it can be set by you via the **ftp** command (see Section 6).

It is very important to note that files on the MSS are not backed up to any other storage device. If you accidentally delete a file, and you do not recover it from the **.trash** subdirectory -- it is GONE! If the UniTree itself suffers a catastrophic hardware failure (such as a disk crash in the caching system) your files will be preserved only if they have been migrated to the tape storage subsystem.

5. Migrated Files vs. Cached Files

The UniTree software is designed to automatically migrate files between the disk cache and the robot tapes, according to a file's creation date and last access or modification date on the MSS. The MSS access date for a file only changes when it is opened via the UNIX **open(2)** system call; merely touching a file has no affect as far as the MSS is concerned. The MSS modification date only changes when a file is modified via the UNIX **write(2)** system call. Files in current use remain cached, while unused files eventually migrate to tape. When a migrated file is accessed, the UniTree will automatically retrieve the file into the disk cache.

A file can reside only in the cache, only on tape, or on both cache and tape. A file's residence is determined by both its MSS creation date and its last MSS access/modification time:

- Any file less than four hours old (i.e., unmodified in the last four hours) will reside only in the disk cache, and is not eligible to be purged.
- After the file is four hours old, a copy of the file will also be written to tape. The disk copy is then eligible to be purged from the disk cache.
- Files will remain in the disk cache until it becomes 90% full. At that time, the UniTree will begin purging eligible files from the cache. Files are selected for purging solely on the time elapsed since last access; the oldest files get purged first. Purging will continue until the cache is less than 80% full. Any file purged from the cache and residing only on the MSS tapes is said to be a migrated file.

Any file modified within the last four hours will remain in cache during a file purge. The four hour limit is a UniTree system parameter which cannot be controlled by the user.

The retrieval time for a file differs greatly between cached files and migrated files. If a file is currently in the cache, you should get immediate response from the computer. If a file has been migrated, you will notice a definite time delay while the UniTree retrieves the file from tape. The load on the UniTree robot is a major factor in the time delay. Tape requests are handled on a first-in-first-out basis. Once your tape request is started, the time delay depends on where the file is in the robot's tape subsystem:

- Is the file on a tape currently in the tape drive? If not, then the tape will have to be fetched by the robot and loaded into the tape drive first.
- Is the tape in one of the 49 robot slots? If not, then a human will have to go get the tape off of a shelf and insert it into a slot.
- Where is the file on the tape? If the tape is full, and the file is at the end of the tape, then the delay will be longer than if the file is at the beginning of the tape.

A delay due to a tape request can vary greatly, but at a minimum will take several minutes.

6. The MSS *ftp* Command

Long delays due to tape accesses can be extremely frustrating, especially when they are unexpected. You can reduce your frustration with the MSS with a modest amount of planning in your work. You should fetch all of the files that you expect to work with into cache before you begin working on them. Since you know that this may take a few minutes, do something else -- get a cup of coffee, read your e-mail, organize your desk. After the retrieval is complete then you can begin work and not be interrupted by tape requests from the MSS.

You can interact directly with the MSS via a special version of the UNIX **ftp** command. If you **ftp** to the MSS and log on, you can find out the disk/migration status of your files, get migrated files into the cache, query your trashcan time-out interval, and set your time-out interval.

To initiate contact directly with the MSS, type **ftp asnmss.asc.edu** from your computer:

```
asncray> ftp asnmss.asc.edu
Connected to asnmss.asc.edu.
7.6.1 Archive FTP server (UniTree Version 1.0) ready.
Name (asnmss.asc.edu:uabxxx01): uabxxx01
7.6.2 Password required for uabxxx01.
Password: *****
7.6.3 User uabxxx01 logged in.
ftp>
```

and log on with your userid and password. Note that you connect to a special port on the MSS; you are *not* connected to the normal ftp port on the RS/6000. The command format above will work for the CRAY, Sun, and RS/6000 machines at ASN but may be different for other machines. If you have difficulty connecting (you get a syntax error from ftp or you do not get the UniTree Version message shown above), you should consult your local documentation for ftp for the machine you are using.

As with any version of **ftp**, you can also get files from (or put files to) the MSS. The use of the **ftp** command is recommended for file transfers to the MSS, because this **ftp** is more efficient than a copy using NFS and does not add system load to either the CRAY or the Sun.

Determining file status

The way to determine the cache/migration status of files is via the **dir** subcommand of **ftp**:

```
ftp> dir
-rw----- 1 xxx group archive 1032 Sep 28 21:13 CHECKSUMS
-rw----- 1 xxx group archive 5862 Sep 28 21:13 FILES.Z
-rw----- 1 xxx group archive 524288 Sep 28 21:16 mit-4.00
-rw----- 1 xxx group archive 524288 Sep 28 21:28 mit-4.04
-rw----- 1 xxx group archive 524288 Sep 28 21:30 mit-4.05
-rw----- 1 xxx group archive 524288 Sep 28 21:32 mit-4.06
-rw----- 1 xxx group disk 524288 Sep 28 21:34 mit-4.07
-rw----- 1 xxx group disk 524288 Sep 28 21:36 mit-4.08
-rw----- 1 xxx group disk 524288 Sep 28 21:45 mit-4.11
```

The output from the **dir** subcommand will be similar to the long listing from the UNIX **ls** command, except that the disk or migration (archive) status of the file will be given after the group designation.

Getting migrated files into the disk cache

Migrated or archived files can be brought back into the disk cache with the **stage** subcommand for **ftp**. The syntax of this statement is:

```
quote stage waittime filename
```

where *filename* is the file you wish to be disk cached, and *waittime* is the time in seconds you wish to wait before the **ftp** prompt returns. A wait time of zero can be specified. Wild cards and multiple file names cannot be used with the **stage** command.

To get the file **mit-4.06** back into the disk cache from the example above, without waiting, you would enter at the **ftp** prompt:

```
ftp> quote stage 0 mit-4.06
```

You could then check the file's disk/migration status later with another **dir** subcommand.

Checking/setting the trashcan time-out interval

You can check and reset the trashcan time-out interval with **ftp** subcommands. The command

```
quote site GTRSH
```

will report your currently set time-out interval in minutes. The default interval is 10 minutes. You can reset this interval with the command:

```
quote site STRSH time
```


where *time* is the time-out interval in minutes.

The following example shows the checking and resetting of the trashcan time-out interval.

```
asncray> ftp asnmss.asc.edu
Connected to asnmss.asc.edu.
7.6.4 Archive FTP server (UniTree Version 1.0) ready.
Name (asnmss.asc.edu:uabxxx01): uabxxx01
7.6.5 Password required for uabxxx01.
Password: *****
7.6.6 User uabxxx01 logged in.
ftp> quote site GTRSH
7.6.7 Trashcan interval is set to 10 minutes.
ftp> quote site STRSH 60
7.6.8 Trashcan interval is set to 60 minutes.
ftp> quit
asncray>
```

In this example, the trashcan interval is increased from the default ten minutes to one hour.

7. Using MSS with the CRAY

Accessing MSS files from the CRAY is inefficient compared to accessing files on CRAY disks such as */tmp* -- the difference in disk access times is a factor of 200 or greater. For efficient computation on the CRAY, you should copy the files which you plan to use to */tmp* first. However, be aware that copying very large (multi-MegaByte) files to or from the MSS can take a long time.

First, make yourself a subdirectory in */tmp* named after your user ID:

```
asncray> mkdir /tmp/uabxxx01
```

Then from the directories of interest on the MSS, copy the files that you need into the CRAY temporary subdirectory. Then *cd* into the temporary directory and begin work:

```
asncray> cp * /tmp/uabxxx01
asncray> cd /tmp/uabxxx01
```

After you finish your work, remember to copy your files back to the MSS in order to preserve them. If you fail to do this, they may be gone from */tmp* the next time that you log on.

What is Administrative Applications?

LANs, laser printers and 4GLs, are here. Why are you still cranking away on a dumb terminal or an XT connected via a modem? This is the Space Grant University and you are filling in forms with a pencil. Why?

Computer Services' Administrative Applications is making a difference on campus. Have you noticed the new schedule/bills being sent out? Students have. Have you seen the new grade sheets? Transcripts? Bids? New technology is being utilized to decrease waste and increase satisfaction. And it can only get better.

Administrative Applications is that flaky bunch in Computer Services who do all the applications programming for the university administration. Every paycheck, transcript, schedule, timetable or phone book that leaves this campus does so because someone in Administrative Applications wrote and maintains some wondrous piece of code accessing some arcane database.

In anticipation of a new mainframe, we are gearing up. We are trying to learn and use software, network, and little, bitty hardware that will get us ready to start using the BIG machine and the suite of packages/applications it will support. Join us in this thrilling move to the hi-tech plateau.

We, like your government, are here to serve you. So let us know what you need; what you want. Is there a job that is paper intensive and do you want to look at ways to put that job on a machine? Does the same piece of paper have to be routed extensively for a process to be complete? Do you see ways your office could be more functionally integrated? We are Computer Services, and our mission is to support the university administration. What have we done for you lately? ■

Downloading Class Rolls

by Malcolm R. Rice

Users within the university community with access to the Student Information System (SIS) are now able to download class roll information for import into other programs such as Dbase III Plus databases and Microsoft Excel spreadsheets.

In order to download a class roll, users must have a valid user-id, password and account number on the Unisys mainframe. These are obtained from Computer Services with a written request issued by the department. Next, the user must have security access to SIS. This can be obtained from the Enrollment Management office, Dr. Ron Koger. Once the user has met the account and security access requirements, all they will have to do is sign-on to SIS and follow the prompts.

Once access to SIS has been established, the user will be presented with a menu of choices. This will differ according to the type of communication the user has. Asynchronous users will see the SIS Short Review Menu while the SIS main menu will be displayed to synchronous users. From the Short Review menu, select option number 5; REVIEW OR PRINT CLASS ROLL. From the

SIS Main Menu the user selects option number 3, REPORTS/PRINTOUT MENU 1, and then selects option number 6, CLASS ROLLS.

Other than the noted differences above, the remaining steps are the same for both types of communication connections. The user is then presented with the CLASS ROLL MENU which lists several choices of class rolls to download. They can either create a file for a single course, a single department or a range of departments. No matter the option the user chooses, the file created contains the course and section number and the following student information: student number, last four digits of the social security number, name, phone numbers, college, class rank, major and anticipated date of graduation. This process creates a comma delimited file for download to a personal computer. The files are downloaded via STEP/PEP or Kermit, depending upon the users' connection to the Unisys mainframe.

Complete details can be found in the *SIS Short Review Users' Guide* available from either the Enrollment Management office or Computer Services Administrative Applications. ■

Mother Says

by Helga Schmedlapp

Greetings and Happy Springtime, Computer People. Mother has been so excited with the rumors of new hardware and software coming into our lives. Can you feel the pulse of new life in the Computer Center? Ah, to computer nerds, nothing is as sweet as a new piece of software to test and use. Mother, naturally, gets more excited with spring scents, but she is not oblivious to the high level of anticipation surrounding her. Have you caught the fever?

Gleanings from E-mail:

Programming is an endless race between the software engineer, who seeks to design increasingly idiot-proof code, and the Universe, which strives to produce even bigger idiots. (The Universe is winning.)

In the beginning was the word. But by the time the second word was added to it, there was trouble. For with it came syntax . . . and you needed version 4.0.

Mother is privileged to be the recipient of wonderful pieces of information. From time to time, individuals will make an effort to enlighten Mother. What follows is such an enlightenment:

The heaviest element known to science was recently discovered by physicists at Turgid University. The element, tentatively named "Administratium", has no protons or electrons and thus has an atomic number of zero.

However, it does have one neutron, 125 assistant neutrons, 75 vice neutrons and 11 vice assistant neutrons. This gives it an atomic mass of 312. These 312 particles are held together in the nucleus by a force that involves the continuous exchange of meson-like particles called morons.

Since it has no electrons, Administratium is inert. However, it can be detected chemically as it impedes every reaction it comes into contact with.

According to the discoverers, a minute amount of Administratium caused one reaction to take over four months to complete when it would normally take less than a second.

Administratium has a normal half-life of approximately 3 years, at which time it does not actually decay, but instead, undergoes a reorganization in which assistant neutrons, vice neutrons, and assistant vice neutrons exchange places. Some studies have shown that the atomic number actually increases after each reorganization.

Research at other laboratories indicate Administratium occurs naturally in the atmosphere. It tends to condense and concentrate at certain parts such as government agencies and computer companies, and can usually be found in the newest, best appointed and maintained organizations.

Scientists point out that Administratium is known to be quite toxic at any concentration and can easily destroy any productive reactions where it is allowed to accumulate. Attempts are being made to determine how Administratium can be controlled to prevent irreversible damage but results are not promising.

Mother ran across a memo that she thought might be appropriate to share with all of her many fine readers during these economic hard times. Even Mother takes time out once and awhile and remembers to be grateful for a job when so many are losing theirs.

MEMO

To: Working Staff
From: Someone Who Cares
Re: Job Griping

Once again I hear mutterings in the hall. Someone is unhappy with their job, or their boss, or their workload, or their salary, or bad hair. Gripping is a great labor tradition. However, it requires a dose of adult behavior to really change anything. Here are some adult considerations.

- 1) What is the problem? Don't start out with a vague unhappiness. Be specific. What is the problem? More than one? Are they related? Write them down!!!
- 2) Talk to your manager. Is there a resolution possible? Don't go off on

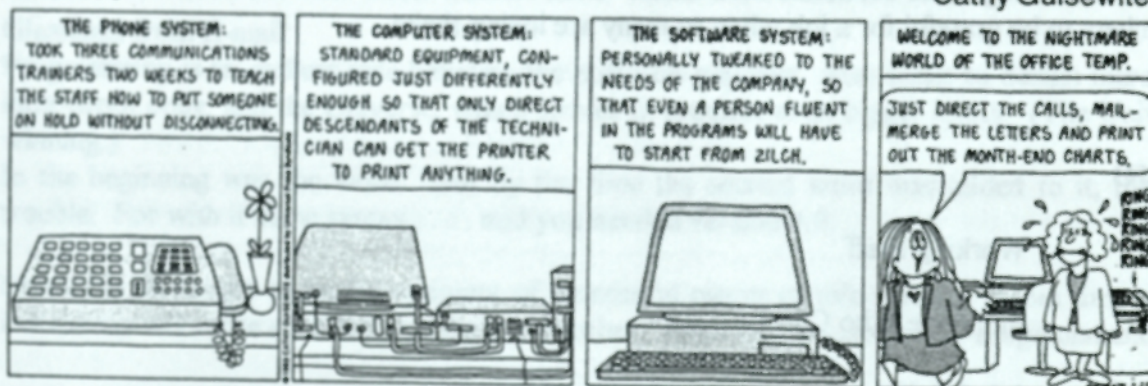
tangents. Stick with the problem(s) you have written down. If you uncover other problems in your discussion, schedule another meeting.

- 3) Be fair. It is human nature to be defensive. Give your manager a chance to respond. If you just attack, neither of you will have accomplished anything.
- 4) Are you breeding more discontent? Why? How does that make this place any nicer to work in? A bird knows not to poop in its own nest.
- 5) Still not satisfied? Go to your manager's manager. Take your list. I guarantee that manager doesn't want to hear about your lumbago or about your dog being sick.
- 6) If all else fails, write a letter and have it put in your personnel file. Document problems and sooner or later they will be resolved. Honest.

Well, Mother has certainly been off her beaten path this issue. Please keep those many card and letter coming in. Mother needs the job. ■

CATHY

Cathy Guisewite



The following is the recently released campus security policy, compiled and written by Rich Hemphill, Network Security Analyst for UAH Computer Services:

Computer Security

Policy

The University relies heavily on the use of electronic data processing systems and computers to meet its operational, financial, and informational requirements. It is essential that these systems and equipment be protected from misuse and unauthorized access. It is, also, essential that the University's computers, and the data that they store and process be operated and maintained in a secure environment and in a responsible manner. The University's policy pertaining to security is as follows. Any violation of this University policy by a University employee or student constitutes theft and/or unauthorized use of University property.

A UAH employee or student, who in the course of his or her employment and/or enrollment intentionally and without proper authorization, directly or indirectly engages in such activities or who damages or destroys any computer, computer system, computer network, program, or data or who causes such acts to occur will be subject to disciplinary action. Such offenses by students constitute non-academic misconduct and will be subject to disciplinary action.

If it appears that the activity is a violation of State or Federal law, the University may report the activity to appropriate law enforcement authorities.

Securing University Owned Computer Resources

All computer equipment, including personal computers, mini-computers, mainframe computer systems, software, files, and computer generated reports are assets of the University and must be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

System Administrator Requirements

All computer assets are assigned to a responsible party. Each application system, and its associated programs and files, are assigned a system administrator who is responsible for ensuring that adequate controls and procedures are in place to protect the integrity of the resources. These controls include application design, testing, computer access security, and proper usage and disposal.

Hardware

Treat your computer equipment as you would any piece of delicate equipment that you depend on. Know the model, serial number, and key characteristics of your equipment. Do not allow the machine to be exposed to elements such as dust, smoke, and/or liquids which

can easily harm the electronic circuitry and other sensitive items such as floppy diskettes or a hard disk.

Software

Before a new software application is installed, a back-up copy should be made of each of the software package's distribution media. After the software is installed, the software's original media and back-up media should be kept in a safe, secure place that is separate from the computer equipment where the software is installed. If you run the application directly from the media, keep the back-up media as your working copy and store the original media in a safe, secure place. You should avoid loaning the original or back-up media of packaged software to other personnel, as unauthorized use of the software may violate copyright or license agreements.

Data

The best protection for your data is to lock it up. Store your storage media, reports, etc. in a secure place. If your computer does not have a lock, do not store sensitive data on the hard disk; use external media so that the media and data can be securely stored in a lockable cabinet. If your computer has security software, you should use it to further protect sensitive data and to inhibit access to certain applications through which sensitive data can be accessed.

If you have printed reports or stored data on your hard disk or external media that you no longer need, get rid of it by following one of the procedures mentioned below:

- Shred and/or dispose of old reports which are no longer needed;
- On a hard disk configuration, delete or erase unneeded files by using the file handling utilities of the computer application used to create the original file; or
- On an external media configuration, delete or erase unneeded files by using the file handling utilities of the computer application used to create the original file. Alternatively, **with caution**, you can reformat the entire media which will erase everything.

Network Use

The UAH Campus Network is a resource that is owned by, and available to, all departments on the UAH campus. Due to the nature of electronic data networking, the potential for harm to the entire network by one errant component is significant. It is important for all to understand that the network will function only if everyone follows a set of basic guidelines for network access and use

Definitions

The UAH Campus Network consists of over 500 nodes and provides inter-departmental and off-campus data communications for academic, research, and administrative applications.

Because of the many access methods, types of storage devices, backup routines, and nodal system administrator requirements, no data on any node should be considered private or secure. The network user is responsible for the integrity and security of files and transmissions.

The network consists of primary and secondary networking equipment. Primary networking equipment is generally those pieces of equipment that are seen by the network as a "whole", including:

- Fiber optic and ethernet cabling.
- Patch panels and premise wiring.
- Transceiver taps and cables.
- Active elements such as bridges, repeaters, and gateways.

Secondary networking equipment includes equipment that is logically on the "user" end of a bridge or gateway, such as workstations and Local Area Networks (LANs).

Rules for Use

- Primary internal network is Ethernet and supported protocols are TCP/IP and DECNET.
- Attachments to the Ethernet backbone shall be made only by UAH Computer Services personnel using previously approved components.
- All primary networking equipment will be considered to be the management responsibility of Computer Services.
- Once primary networking equipment is installed, it becomes the responsibility of Computer Services and may not be relocated by the user department.
- Internet Protocol (IP) and DECNET addresses will be assigned only by Computer Services. Those wishing an address assignment must complete the UAH Address Request Form available from Computer Services.
- Any inter-department network applications must be coordinated with Computer Services
- Failure to comply with this network policy will result in removal of the offending equipment from the network.

Documentation

The best protection for your computer documentation is to store it in a secure, but easily accessible place. For commercial or purchased software, copying documentation may be a copyright violation. Therefore, DO NOT make any copies of vendor supplied

documentation. If you have any questions regarding this policy, contact the Vendor or Network Security personnel for clarification.

Documentation which supports a recurring report or custom application which has been developed within the department can, and should be, reproduced. A reproduction of the original should be labeled as the working copy; this is the copy which is used by users. The original documentation should be stored in a separate location which is safe and secure from any chance of destruction.

User Access of Computer Systems

All users are held accountable for all actions performed on the computer systems with their log-on ID (i.e., user name and password).

Users are only to perform functions on the computer systems for which they are authorized, and in direct support of their job function.

The following constitute a violation of University policy:

- Deliberate, unauthorized attempts to access or use the University's computers, computer facilities, networks, systems, programs, or data or the unauthorized manipulation of the University's computer systems, programs, or data.
- Deliberate, unauthorized use of UAH facilities or equipment to access non-UAH computers.
- Deliberate, unauthorized activity which causes UAH computers, computer facilities, systems, programs, or data to be accessed or used.
- Deliberate activity (conducted in the course of one's employment with the University or in the course of one's enrollment as a student at the University) which causes non-UAH owned computers, computer facilities, systems, programs, or data to be accessed or used in an unauthorized manner.

Password Administration

Passwords are to be kept confidential. Only the individual user to whom the log-on ID is assigned is to know the password. Disclosure of the password is a serious security violation and may result in loss of systems access privileges, and possible disciplinary actions.

Passwords are not to be programmed into a computer, or recorded anywhere else that someone may find and use them. When creating a password, it is important not to use one that may be easily guessed, like a common dictionary word or name of a relative or pet. The best passwords are purely random combinations of letters, digits, numbers, and punctuation.

Security Violation Administration

Security violations should be monitored and reported to Network Security personnel.

Contingency Planning - Back-up and Recovery

The System Administrator or individual computer user should ensure that recovery systems are in place so that all critical applications and data is recoverable without seriously hampering operations.

Data Security

Data should be kept secure for a host of reasons. However, the level of data security varies depending upon the type of information. Some information is for internal use, while other information is publicly disclosed (e.g. Annual Reports, Quarterly Reports, etc.). Of the data that is for internal use only, there are varying levels of security based on its potential effect.

Level 1 Data: Confidential Information

Level 1 data represents very important and highly sensitive material. It is used mostly by upper level management and is for internal use only. Unauthorized disclosure, modification, or destruction of this information could cause serious damage to the University and/or its clients. Ownership of Level 1 data should be well established and assigned to responsible persons who will maintain the safety, viability, and integrity of the data.

Examples of Level 1 data include: strategic planning documents, program marketing materials, accounting reports, system access passwords, and data file encryption keys.

Level 1 data requires strict access control for which passwords should be granted and an access log maintained. Back-up procedures should ensure that the material can be re-created in case it is damaged or destroyed for any reason. The owner should give, in writing, authorization for any actions such as duplication, dissemination, or destruction of this level of data. The owner should maintain absolute control over the data management functions such as update, storage, and all modes of disposal. Restore and recovery procedures should be well documented and proven to work.

Level 2 Data: Restricted Information

Level 2 data represents important data to the University. Its dispersal, destruction, and/or modification could result in serious losses. This information is for internal use only. Typically, this level of data is used by upper management personnel. Users of this level of information include different departments or affiliates of the University. Such information would include information on students, the financial records of different departments, personnel or payroll records, and budget information. Even though many people are authorized to have access to this level of information, access must be restricted. Access should be granted in writing and with the owner's full understanding of the intended use of the data. Access should only be given to those with established business needs. Disposal of this information must be done in a manner such that the material is no longer legible or recoverable. In order to ensure on-line security, access control should be implemented via passwords for both system access and application execution.

Level 3 Data: Internal Use Information

Level 3 data is important institutional information and is meant for internal use only. Employee access to this level of data is not restricted, but the data requires the owner's approval for outside distribution. The data normally included in this level includes the local operations manual, corporate policy and procedures, inter-office notes, and the company telephone directory. The storage of this information is the responsibility of each employee, since the amount of information is somewhat larger than in other levels. This level of material can be disposed of in any of the routine methods normally used by the company.

Level 4 Data: Unclassified Information

Level 4 data represents information that is typically available to the general public. It requires no restrictions and no special protection procedures. This information is normally accessed, but not modified, by employees and/or students. No special procedures apply for accessing, storing, or disposing of this level of data. Examples of this information include: annual and quarterly reports, internal procedures, and University-wide memos.

Dial-Up Access

Access to the personal computers, mini-computers, or mainframe computer systems via dial-up phone lines is controlled by security systems to provide an acceptable level of protection from unauthorized entry. Access via dial-up is accepted as a normal avenue for system access.

Copyright Laws/Proprietary Software

All software is to be used in accordance with the manufacturers lease, license, and/or purchase agreements.

Responsibilities

Users, user management, security administrators, and systems development are all responsible for maintaining security controls. The following delineates their specific duties and responsibilities.

User

All users are responsible for adoption and active support of security procedures, including:

- Keeping their password confidential;
- Reporting all known security exposures and violations to their management; and
- Using the computer systems only in support of their authorized job responsibilities.

User Management

User management is responsible for overseeing their employees' use of computer systems, including:

- Reviewing and approving all requests for changing their employees access authorizations;
- Initiating security change requests to keep employees' security record current with their positions and job functions, including terminations and transfers;
- Providing employees with the training needed to properly use the computer systems; and
- Reporting any known security violations to Network Security personnel.

Security Administrator

The security administrator is responsible for working with user management to develop and implement prudent security policies, procedures, and controls, including:

- Providing basic security support for all systems;
- Advising in the implementation of security controls on all systems, from the point of system design, through testing and production implementation;
- Providing comprehensive information about security controls affecting system users and application systems; and
- Providing security support for all system users.

Systems Development

Systems development is responsible for including reasonable security and back-up controls in the applications being developed and maintained, including:

- Providing assistance in the identification and classification of computer resources;
- Working with user areas and security administration to develop and integrate security controls into all systems, from the point of system design, through testing and production implementation;
- Creating comprehensive documentation on application design, program logic, back-up and recovery procedures, internal application security; security controls and interdependence on other systems; and
- Thoroughly testing all systems for accuracy and for proper security and disaster recovery controls.

Credits

Portions of this document were taken from the PC HandiGuide Manual, Personal Computer Policies and Procedures Manual, Version 4.0, and modified to fit the needs of Computer Services at the University of Alabama in Huntsville.

Is Your PC Cable Ready?

by Frank Gossett

CATV PC? Not exactly. Although possible, the focus of this article is about data delivery to the PCs rather than images seen on television.

As technology becomes more refined, our perception of computing becomes more abstract. Where the vehicle of delivery was once a single computer (e.g. PC, mainframe, etc...), it is now becoming "The Network". Just as the computer requires its components (disks, memory, power supply, etc...) to work together to produce the functions we can't live without, so must the network via a relationship of cooperating computers. Whether we like this trend or deny its presence, the models for cooperative computing continue to develop. Though the underlying details are often cursed, more often than not the results are praised.

So the question becomes, "What do I buy to ensure current and future benefits from network services at UAH (...Or paraphrased, "How do I help prevent my computer from being a square peg in tomorrow's round hole?")?". Two possible configurations for Spring '93 are listed below. These suggestions are based on current support level experience with maximum campus interoperability objectives.

A. Assuming you do not currently have a network interface of some kind in place, A Macintosh LC III microcomputer should have:

- 8MB of RAM (at least)
- 80 Megabytes of fixed disk (at least)
- 1 Assante or Apple Ethernet Adapter (10BaseT and/or 10Base2)
- Network software appropriate for your location and recommended by UAH Computer Services (e.g. NCSA Telnet, etc...).

B. IBM compatible 486 microcomputers should have

- 8MB of RAM (at least)
- 212 Megabytes of fixed disk (at least)
- 1 SMC Elite16 Ethernet Adapter (10BaseT or 10Base2)
- Network software appropriate for your location and recommended by UAH Computer Services (e.g. NCSA Telnet, etc...).

Note that the previous checklists are only valid if you have a need to connect to other computers. The suggestions above also do not address other subsystems required for day-to-day tasks (e.g. tape backup units, monitors, etc...).

Some example questions that need to be resolved before determining your pre-purchase configurations follow:

- Does my building have network access?

- How do I connect to the campus network from my office?
- How can I tell if I have a network connection already?
- What's a network?


If you have any questions about configuring network-ready PCs, please call UAH Computer Services, 895-6347/Option #1.

DEC CampusWide Software License Grant

UAH and Digital Equipment Corporation have entered into an agreement which gives VAX and Ultrix (UNIX) software to the university for an extremely low cost to Computer Services and no cost to the user. In addition to the free software, discounts of between 10% and 40% on all hardware is available.

All VAX software in the Campus-wide Software License Grant (CSLG) program is available for use on licensed VAX and Ultrix equipment that is maintained by the individual department. This includes all operating system updates, language compilers, case tools, PC and Macintosh integration products (server only), management tools, etc. The list contains over 600 product licenses.

Computer Services has manuals available for a subset of the products on a 48 hour checkout basis. However, we encourage users to purchase their own set of documents. The program includes software telephone support and updates through UAH Computer Services.

The entire program has a value of well over thirteen million dollars and is a way for the VAX community to maintain current software levels. It is open to any VAX that is titled to UAH, that has previously purchased a VMS commercial operating license, and is used in legitimate research or administrative functions. Machines purchased for government contracts which reside off campus are not eligible. For more information about the program and a complete listing of the products, contact Computer Services at 895-6347 x 231. 

Software Piracy

Reprinted from:

Campus Computing, University Computing Services University of British Columbia January 1992 vol. 7, no. 1 By Teresa Tenisci (ISM) (teresa_tenisci@mtsa.ubc.ca) and Wendy Alexander (UCS) (alexande@ucs.ubc.ca)

When we speak of pirates in today's world, two different visions come to mind. The first is of a latter-day swashbuckling ruffian who captures cargo ships and steals the riches and wealth aboard for himself. The second is of a person who copies software from a source to their own PC, without purchasing it from a legal vendor. We may see both as underdogs, fighting the injustice of "the system," while remaining worthy at heart, and therefore somehow admirable. No wonder

software piracy is not viewed as a crime by most people. In fact, software piracy is a crime. It is theft.

When a software package is purchased from a legal vendor, a contract exists between the vendor and the purchaser. This contract, called a licence, can be found in various places: in the instruction manuals, other documentation, or on the disk itself. Most people believe that once they have purchased software, they own it. This is not quite true. In fact, what has been purchased is the licence which allows the purchaser to use the product. The software company still owns the software. This lack of understanding often leads to breaches of the contract through software piracy, and in many cases the culprits are not even aware of the illegalities of their actions. Sometimes, just breaking the seal of a disk package constitutes a legal and binding acceptance of the licence's conditions.

Don't make UBC the target for the next search warrant. The embarrassment that would be caused by a lawsuit would be damaging to the reputation of the University, and the fines can be very expensive. Don't be fooled into thinking that only the University will be liable and have to pay. Depending on policies in place within your department, you too, might be liable.

What follows are some common situations that will test your knowledge of what is legal and what is not when it comes to software duplication.

Situation #1: A software program has been purchased by an office for one of its employees. Other employees in the same office hear of the program and discover that it would be a great help to them in their work. Can legal copies be made?

Answer: No, legal copies cannot be made. Many people make this mistake, believing that as long as the program is for company business, the use of it within the workplace is legal. Most licence agreements require that each machine or workstation that uses the program must have a purchased copy of that program.

Situation #2: A computer which "belonged" to the employee you are replacing is now yours. All sorts of wonderful programs are on it and you assume they are legal copies. If you are audited and are found to have illegal software on your machine, are you responsible?

Answer: You may be responsible, depending on policies within your department. Just because somebody else put the software on the machine doesn't mean that you are blameless. Essentially, you turned a blind eye and benefited from the existence of the software on the machine. Ways to determine whether or not your software is legal are: check to see if official documentation exists for your machine; check to see if there are any official diskettes for the program; check for official templates on your computer keyboard. If none of these three exists, be prepared to find out that the software is illegal. You may want to speak with the person in your department who keeps track of purchasing software for more information on the programs installed on your machine.

Situation #3: The office operates on a network. Since one person has a legal copy of a software program, and has installed it on the network, everyone is allowed to use it. True or False?

Answer: Either answer may be correct, depending on what the software licence says. Some licences are strict and insist that every person who uses a program, whether it be on a network or not, must purchase the program. Some software companies sell site licences, and these allow everyone on the network to use the program without purchasing copies for each individual who will use it.

Situation #4: An update for your spreadsheet program arrives. Your coworker has been asking you for a copy of the program, but you know that it is illegal so you refused. But now that the new version has arrived, and you have no need for the old version, can you give it to your coworker?

Answer: No. Updates are defined as enhancements to the original package that you purchased. Once the package has been updated, the old package should be destroyed or used solely as a backup.

Situation #5: You have a big presentation to give tomorrow and, as five o'clock rolls around, you realize that you have to be home to babysit your children. Once the kids are settled in bed, can you use the software from the office on your home machine?

Answer: Maybe. Again, it depends on what the software licence says. Some licences say that software can be used both at home and at the office. Some say that the program can be used on several machines, provided that no two are running at the same time. Some programs are very restrictive, and say that the program can only be used on one machine. If you don't have access to the licence, or if you find it ambiguous or unclear, make sure you check with someone such as a technical support person, about the details before you copy anything. If you find yourself in a situation like this and don't know the answer, someone else does. The Software Publishers Association operates a tollfree hotline number through which you can access information about how to order an antipiracy video or a self-audit kit, or just get some anti-piracy information. The number is: 1-800-388-7478.

If you are interested in viewing the video about software piracy, it is called *It's Not Worth the Risk*.

UAH COMPUTER LABS

Location	Hardware	Software	Notes
ASB 214	21 Sperry XT 21 Draft Printers	First Choice; Grammatik IV; Lotus 1-2-3 ; TurboBasic; Cobol ; GW Basic; GINO; LINDO; MyStat; SysStat; The Data Analyst; Layout; Generic CADD; First Publisher; Flow Charting III; XDB-SQL; student version of DBase III and RBase; VP Expert	<u>ASB Hours:</u> M-Th 8a-10p F 8a-5:30p ; S 10a-5p Sun 1p-5p Assist. -6604 Rm 214
ASB 215	21 Zenith XT 21 Draft Printers 1 MacIntosh	terminals for UNIX and VMS, Access to Alabama Supercomputer Network (ASN)	<u>CSB Hours:</u> M-F 8a-11p S 9a-5p; Sun 12-7p
CSB 127	21 DEC VT-320 1 high-speed printer	UNIX, Open Windows, Interleaf, Internet access	<u>System Administrator</u> CS Dept. -6088 Jill Parker - 6904, CSB 128
CSB 143	1 SUN 4/280 1 VAX 3300	VMS, Ada Turbo Pascal; Turbo C++; Meridian Ada; Fortran; Modula2; Assembly, Lisp, Prolog, Snobol (on Novell Netware)	<u>Lab Assistants</u> Aparna Kakarla Donald Jackson CSB 126, - 6542
CSB 157	9 TI 286 PC's 4 clone 386 PC's 18 clone 486 PC's 2 dot matrix printers	- accessible from Novell network - access to Sun system and Internet - access to Sun system and Internet - access to Sun system and Internet	
CSB 156	2 Sun SPARCstation IPC 2 Sun SPARCstation SLC 1 SUN 3/470 1 MacIntosh IIX 1 Apple Laserwriter II 1 Sun laserwriter IIntx	Microsoft Word, Microsoft Excel - accessible from MacIntosh - accessible from Sun system - access to Sun system and Internet	
CSB 158	15 Sun SPARCstation 1+	Fortran 77; Pascal; C; ANSYS (finite element analysis); PHOENICS (fluid flow analysis) Fortran; Pascal Access to ASN	<u>EB Hours:</u> M-Th 8a-10:30p Fri 8a-4p Sat 10a-4p Don Milligan -6132 EB246
EB 122	1 HP 9000/6 stations 8 PC Clones	<u>Restricted Research Lab</u> <u>Restricted to EE301, EE303, EE305 students</u> Intergraph Software <u>Restricted Lab</u>	EB122, EB205, EB216 and EB 225 on EB Novell LAN
EB 205	12 clone 386 6 printers	<u>Restricted for graduate students only</u> <u>Restricted for graduate students only</u>	
EB 216	7 Sun SPARCstations	Works; Word; Word Finder; Hypercard; Wingz; Powerpoint; More II; MacDraw II; MacPaint II; Superpaint; AutoMac III; Virus Detection	<u>Lib Hours:</u> Circ Desk -6530 Liz Pollard -6313
EB 225/227	24 Clone AT	Turbo Pascal; Turbo C; Fortran; MuMath CalcAide	<u>MDH Hours:</u> M-F 8:15a-4:45p Dean's ofc -6605
EB 246	8 Interpro 220 1 Plotter	First Choice; SYSTAT; and MYSTAT available in all MH Labs	<u>MH Hours:</u> M-Th 8:30a-8p Fri 8:30a-5p Sat 8:30a-1p
EB 262	12 clone AT 386	EasyGraph ; Plot 10 TCS & AGII ; Disspla ; Disspla GKS ; Movie.BYU ; IGL	Dr. Sullins -6191 <u>RI Hours:</u> 24 Hours - 7 Days Comp Serv -6347 Access to ASN Access to Mainframe
EB 264	12 clone AT 386		
LIB Circ Desk	6 Macintosh SE		
Valid UAH	1 Draft Printer		
ID Req'd	1 Laser Printer		
MDH 213	16 Dos PC's		
MH 114	2 Sperry XT		
MH 118	15 Sperry XT 15 Draft Printers		
MH 204	21 Sperry XT 21 Draft Printers		
RI M20	2 41xx TEK Term'l 1 4692S Copier syst 1 4207 TEK Term 1 4170 Processor 1 UTS-20 Term'l 1 HP LaserJet 1 PC clone		
RI M25	16 UTS-20 Term'l 1 VT-320 Term'l 3 GVT-1220 Term'l 1 Sperry PC	Cobol ; Assembler ; Basic ; Fortran ; Pascal ; QLP ; PALS ; IMSL ; SPSSx ; other mainframe software	Access to ASN Access to Mainframe
UC 112	16 UTS-20 Term'l 2 Draft Printers	Access to Univac 2200/402 mainframe software via UTS Terminals	<u>UC Hours:</u> M-Th 8a-9p Fri 8a-6p

UAH COMPUTER LABS - RESTRICTED

<u>Location</u>	<u>Hardware</u>	<u>Software</u>	<u>Notes</u>
NB 4th Floor	7 Zenith XT 2 Sperry XT 12 Draft Printers 2 Laser Disk Player 7 Zenith Laptop 5 Zenith Portable	Computer assisted instruction on many health related topics ; Budgeting ; Staffing ; Biostatistics; Speed Reading ; Pascal ; Professional Electronic Recruiting Exchange (PERX System) <u>Restricted to Nursing Students Only</u>	<u>NB Hours:</u> M-F 8:15-5p Evening hours vary Jean Ennis 5-6512
MDH214	1 Sun 4/260 with 2 workstations	<u>Restricted Math Lab</u>	Dr. Epperson -6609
OB 108	2 HP9000	<u>Restricted Optics Lab</u>	Dr. James Hadaway - OB400Q
OB 318	6 clone PC's	Mathematica, MathCADD, MS C, Pascal, Sigma Plot, Power Point <u>Restricted Physics Lab</u> <u>Restricted Aeronomy Lab</u>	Dr. Russell Chipman
OB 349	VAX 4000 2 PC clones		Tony Orme
OB 447	Micro VAX II with 4 term'ls 1 MacIntosh II	VMSoperating system, Code V Lens Design Pro, Synopsys Lens Design <u>Restricted Optics Lab for Lens Design</u>	Dr. Russell Chipman

UNISYS 2200/402 COMPUTING FACILITIES

Major Hardware

- Two Instruction Processors (IP). Perform logical, arithmetic and instruction sequencing operations and is sometimes referred to as a central processing unit.
- Three Input/Output Processors (IOP) to control I/O operations between peripherals and the system.
- Two Main Storage Units (MSU) each consisting of and interface, control logic and 4 megawords of random access storage.
- One common I/O Processor (CIOP) to provide system initialization and microcode loading.

Peripheral Equipment

- Two M9270 disk subsystems with a total 14.61 gigabytes of storage.
- Two Uniservo 34 Tape Drives for 9-Track, 1600/6250 BPI.
- Four Uniservo 36 Tape Drives for 9-Track, 1600/6250 BPI.
- Two 9246 Printers (2000 links/min).
- One Distributed Communications Processor (DCP-40) with 32 Synchronous lines, two 9600 baud lines for graphics use plus 16 Asynchronous lines connected to a DEC Reverse LAT terminal server.
- One Bus-Tech Inc. Ethernet Control unit (HLC) for TCP/IP access.

Software

The software system is based on an Executive known as the 1100 Operating System. The resident 1100 system includes:

COBOL	PASCAL	FURPUR	FORTRAN
BASIC	DOC	PALS	KERMIT
ED	QLP-1100	DPS-1100	ELT
FAS	SSG	CML	SYSLIB
FLIT	MetaAssembler	SORT/MERGE	PCIOS
PDP	PMD	DMS	

Other available libraries include:

- Statistical Package for the Social Sciences (SPSSX).
- Tektronix PLOT 10 Software, TCS, AG2, IGL, and Easygraph DISSPLA graphics.
- Unisys Mathematical Subroutines (Math Pack).
- Unisys Statistical Subroutines (Stat Pack).
- International Mathematical and Statistical Library (IMSL).
- Biomedical Statistical Library (BMDP).
- Ordinary Differential Equations System (ODEPACK).
- SYSTAT, SYSGRAPH, NCAR.
- Harvard Graphics.
- Campus Software Library Grant (DEC).

A User's Guide is available in machine-readable form. A GUIDE Processor is available to users for extracting and printing material from the Guide. The Computer Services staff is available to consult with the university community on problems associated with use of the Center.

COMPUTER SERVICES SOFTWARE SUPPORT POLICY REV 1.6

Recognizing the dynamic needs and complexity of large organizational support, it is this policy's intention to provide a framework for the best information systems' support possible with our current resources and strategic perspective.

The following UAH Computer Services' supported products represent a movement toward cooperating software with more consistent organization-wide user interfaces. This software standardization facilitates cost effective support and information exchange between elements of the university.

- UNISYS OS1100 operating system, utilities and applications.
- VMS operating system, utilities and application components of the DEC Campus Site License Grant program.
- The Unix operating system.
- NOVELL NETWARE 386
- Programming language compilers including Assembly, C, C++, COBOL, FORTRAN, and Pascal.
- NCAR graphics for CRAY and VAX systems.
- DISSPLA graphics for CRAY and UNISYS 1100 systems.
- SPSSX statistics for Cray and Unisys systems.
- SYSTAT/SYGRAPH statistics for DOS environments.
- Microsoft WORD, EXCEL and POWER POINT for the DOS Windows and Macintosh environments.

Note!! Given the variety of software available on the university's diverse hardware platforms, it is recommended that the computer user community consult UAH Computer Services prior to resource acquisition to determine the compatibility and level of support available.

Software support is provided by consultants located in The Research Institute rooms M-30 and M-21. Phone assistance may be obtained by calling 895-6347 option 4. Normal consulting hours are 8:30 A.M. to 5:00 P.M. Monday through Friday.

The University of Alabama in Huntsville acknowledges the rights of computer software developers and prohibits the copying of licensed or copyrighted software without permission from the licensing authority. Consequently, technical support for illegally acquired software products will not be provided.

Network Address Request Form Completion Instructions

Refer to the Network Address Request Form for sections of the form described herein.

CONTACT INFORMATION:

Name: The name of the actual user of the workstation or the system administrator if the machine is a multi-user platform.

Department: Department to which the machine belongs. Be as explicit as possible.

Mailing Address: The Campus mailing address of the user. Include room numbers.

E-Mail Address: The electronic mailing address of the primary user or system administrator.

Phone Number: Entire campus phone number including extension.

EQUIPMENT INFORMATION:

Type of Equipment: The manufacturer, make and model of the machine. Include any model numbers.

Equipment Location: The physical location of the machine. Include site, if off campus, building, room number, and section number if applicable.

Operating system: Type of operating system in use on the machine.

Comm. Hardware: Type of interface in use to connect to the network.

Comm. Software: Type of communications software used to access network.

CONNECTION INFORMATION:

Type of connection: Check appropriate selection. Give any additional information requested based on selection (i.e. give the ethernet address or serial connection scheme used to connect to the network).

NODE NAME INFORMATION:

Internet Node Name: The name by which the machine will be identified on the network. This name can be as long as desired. If any subdomain (i.e. CS.UAH.EDU) is desired, supply the information as part of the node name.

DECNET Nodename: The decnet node name desired (max of six characters).

The number will be assigned by Computer Services personnel and the user listed in the contact information section will be notified by phone or E-mail of the assignment.

**UAH Network Services
Network Address Request Form**

Date: _____

SEND TO: Rich Hemphill
Computer Services
Research Institute

DECNET: ASNUAH::UAHRGH01
INTERNET: RHEMP@UAHIS1.UAH.EDU
VOICE: (205) 895-6347

CONTACT INFORMATION

Name: _____

Department: _____

Mailing Address: _____

E-Mail Address: _____

Phone Number: _____

EQUIPMENT INFORMATION

Type of Equipment: _____

Equipment location: _____

Operating System: _____

Comm. Hardware: _____

Comm. Software: _____

CONNECTION INFORMATION

Type of connection:

Ethernet: () Ethernet Address: _____
(e.g. 00-00-00-00-00-00)

Serial: () Connected To: _____

Connection Speed: _____

Other: () Describe: _____

NODE NAME INFORMATION

Internet Nodename: _____ (.UAH.EDU)

DECNET Nodename: _____
(If applicable, 6 characters)

PROCESSING INFORMATION TO BE COMPLETED BY NETWORK SERVICES

IP ADDRESS: _____ DECNET Address: _____

Date Completed: _____

Mailing List Update Form

Please delete my name from the Newsletter mailing list:

☐

Please add my name to the Newsletter mailing list:

☐

Please change the following information:

☐

Name:

Address:

An Affirmative Action/Equal Opportunity Institution



The University Of Alabama In Huntsville
Computer Services
Huntsville, Alabama 35899

Nonprofit Org.
U.S. Postage
Paid
Huntsville, AL
35899
Permit No. 283

Library
Serials Dept.
LIB