United States
Environmental Protection
Agency

Office of Administration
and Resources Management
National Data Processing Division
Research Triangle Park, NC 27711

397/001
December 4, 1989

EPA

LAN Administrator's Technical Reference Guide

Preface

This manual is designed to provide the Local Area Network (LAN) Administrator with procedures and operational guidelines for properly installing and maintaining Agency-standard LAN's.

The LAN Administrator's Technical Reference Guide has been divided into four sections for each topic were applicable. These are: Overview, Installation, Operation, and Troubleshooting. The Overview section has been written in a manner which can be understood by either technical or nontechnical readers, while the other sections are primarily written for Technical Administrators.

As new applications and system software are supported by the EPA National Data Processing Division, they will be added to the reference manual. Annual updates will be made to this manual.

Table of Contents

List of Figures

1. NETWARE ASYNCHRONOUS COMMUNICATIONS SERVER

OVERVIEW

The NetWare Asynchronous Communications Server (NACS) is the software which provides LAN network workstations with the ability to share communications lines: either dial-up phone lines with modems or directly-connected lines to other asynchronous devices, such as data switches. A communications server is sometimes referred to as a Gateway, because it provides access to other (often dissimilar) devices that are not directly connected to the network.

If a person working at a PC wants to communicate with another computer through a modem, the modem would have to be directly connected to one of the PC's communications ports. The user would then dial the modem and establish the desired connection. In a network environment, having a modem on every PC would be too expensive. Instead, a gateway server is used to provide users access to a "pool" of resources which they share; providing asynchronous communications access for all users at a minimum cost.

The NACS gateway consists of up to four add-on boards that fit into an IBM or compatible PC, as well as special control software. Each add-on board can provide four ports for connection to modems or to a data switch. This hardware and software combination allows a PC to function as a gateway for network users to gain access to outside asynchronous devices. It also provides users with the capability of dialing into their workstations on the LAN giving them access to all of their LAN files from a remote location.

Documentation

The document provided with the NACS gateway software package is the NetWare Asynchronous Communications Server Supervisor Manual (May 1988/Rev 1.00).

INSTALLATION

Installation of the NACS gateway is completed in five steps:

1. Selection/configuration of a gateway PC.
2. Installation/configuration of the NACS software on the gateway PC.
3. Installation of the add-on boards on the gateway PC.
4. Installation of the control software on the file server.
5. Modification/Creation of the Script files.

Select/Configure the Gateway PC

Selection of the gateway PC is very important. If only one add-on board is to be used, most IBM or compatible PC's may be used. If, however, more than one add-on board is to be used, only two types of machines have been successfully used in the Agency: an IBM XT with 256kb of memory and an Epson Equity III with 256kb of memory. (The gateway PC DOES NOT require a hard disk.) The Epson memory configuration may be changed by moving jumper switches in the machine and running the set-up software. On the IBM XT, the memory may be physically removed from the machine. Refer to the manuals provided by the manufacturer of each machine for specifics.

Install Software on Gateway PC

Installation of the NACS software on the gateway PC (NACS Manual, Page 2-4) consists of creating a boot disk for use on the gateway, as well as configuring each add-on board to be installed in the gateway. Since a hard disk is not required on the gateway, the example given will use a floppy disk.

1. Create a boot disk as you would normally, leaving out all DOS files with the exception of EDLIN, since they are not required for gateway operation. Be sure to include on the boot disk, however, any "xxxx.SYS" files you may require.
2. On the boot disk, create the config.sys file as you would for a workstation. Do the same for the autoexec.bat file.

3. Copy the entire NACS program diskette to the boot disk. The autoexec.bat and config.sys files used on the NDPD Epson which runs DOS 3.1 are as follows:

CONFIG.SYS	AUTOEXEC.BAT
device=dxma0mod.sys	path a:
device=dxmc0mod.sys	prompt=pg
files=20	nacs
buffers=20	

4. You are now ready to configure the NACS program to recognize the WNIM+ boards that you will install in the next step. At this point you will select the base I/O address and the Memory segment address for each board you will install in the gateway. When testing the NACS gateway on an Epson Equity III configured with 256KB of memory, the following settings were successfully used:

BASE I/O	MEMORY
290	7000
280	6000
2A0	8000
2B0	9000

5. You can now run the program that will configure the NACS program to recognize the WNIM board(s) you will be using. To do this, using the floppy disk you created earlier, key in the following:

NACSINST NACS.EXE

When the program loads the required configuration and name files, you will receive the prompt to keyin "B" to examine or change the board configuration or "E" to change the name or port defaults. At this time, key in "B". You will now be prompted as to the course of action you wish to take in configuring each board you will use (NACS Manual, Pages 2-5, 2-8). As each board setting is selected, the switch setting that must be made on each board is displayed. Make a note of the switch settings you select so the proper settings can be made on the boards during installation of the boards in the gateway.

6. After you have configured the required boards, you will be returned to the "B" or "E" prompt mentioned above. You must now configure each port name and the software configuration parameters for each port (NACS Manual, Pages 2-9, 2-17). Answer the prompt with an "E". The screen will display the default settings for the NACS Server Name, the specific and logical names for each port, as well as the receive, transmit, and timeout (ITO) values for each port. As you can see in the example given on page 2-11 of the NACS Manual, the NACS gateway is called NACS01. Each port has a specific name of NACS00PORTxx, where xx is 00-15. The general name for all ports is LINE. This is very important for these names greatly simplify the manner in which a port is selected from the workstation when gateway access is required. In the example given, all ports are configured identically. The configuration you will be using may or may not be similar.

7. As an example, say that Ports 0 through 3 will remain unchanged. We will change Ports 4 through 7 so they will be configured on a data switch, such as the DEVELCON at NCC. In this case the parameters will have to be changed. At the prompt enter "4" to change Port 4 (NACS Manual, Pages 2-12). Following the example in the manual, you should change the general name and the receive and transmit parameters. Enter "SWITCH" for the general name. Again, following the prompt, you would change both the receive and transmit parameters to reflect the following: Baud Rate 9600, Data Bits 7, Stop bits 1, Parity even. Set the inactivity timeout (ITO). This will clear and free a port for use if no activity occurs on the line for the specified timeout period in minutes. The value you specify will be your choice. However, do not set it so low that the user will not have time to complete a short phone call without losing his gateway connection. Also, Do NOT set a timeout value on a port which will be used for the ANYWARE dial-in feature. If a user wishes to access their workstation PC on a Sunday, he could not start ANYWARE on Friday before leaving work without the timeout value expiring, rendering the port unusable for ANYWARE. Remember, these are only EXAMPLES. Your actual configuration will depend on the types of lines you attach to your gateway.

Given that the gateway has a set of ports configured with the general name of LINE and another set with the general name of SWITCH, port selection becomes very simple. This will be covered in more detail in the section on installing control software on the file server.

8. After all required configuration changes have been made, exit the NACSINST program, saving the configuration as prompted on the screen.

Install Add-On Boards on Gateway PC

It is now time to install the WNIM boards into the gateway PC (NACS Manual, Pages 3-2, 3-8). During installation of the NACS software on the PC, you were instructed to make note of the switch settings you selected during the configuration process. Following the instructions in the NACS Manual, set the switch settings for each board being installed in accordance with the above mentioned list. Following instructions in the manual, install each WNIM board into the gateway PC.

Install Control Software on File Server

Installation of the software on the file server consists of loading the NASI interface software and the ASCOMIV and ANYWARE software on the file server. To accomplish this, you must be logged on as Supervisor on the file server where the products are to be installed. The installation must be done on the server, not on a workstation hard disk.

The installation process will create a directory called SYS:\NASI-APPS, if one does not already exist. All files created as part of the installation will be in this directory. The directory hierarchy displays as follows when installation is complete:

```
SYS:NASIAPPS –
              |-CONTROL
              |-ASCOMIV -
                        |-SCRIPT
              |-ANYWARE
              |-USERS -
                      |-(USER ID'S)
```

With the ANYWARE and the ASCOMIV products, you will receive a diskette labeled NACS/NASI Applications Installation Diskette.

The diskettes with each of the above mentioned products are identical, so either can be used. (Be sure to make copies of the diskettes to use during installation.) Also included is the NACS/-NASI Applications Installation Supplement (Aug 1988/Rev 3.00). This manual is the one referenced during this installation procedure. Place the originals in a safe place.)

1. Place the installation diskette in drive A: and keyin the following:

   INSTALL

   A screen similar to the one on Page 2-3 of the manual will be displayed. Answer YES to the message if you wish to continue the installation process. Continue to follow the prompts until the AVAILABLE TOPICS window is displayed as shown on Page 2-6. If you wish to install ASCOMIV or ANYWARE, select the INSTALL PRODUCT option. You will be instructed, as shown on Page 2-7, to install the product diskette. Install either the ASCOMIV or ANYWARE diskette in drive A: and follow the instructions. If you must install both ASCOMIV and ANYWARE, this Install Product option must be run once for each product.

2. After the products are installed, you must identify the users of the gateway applications. To do this, select the Modify Product Users option when it is displayed. The first display you receive will be the users already allowed access to the gateway. If you wish to add a user that is not on the list, hit the <Insert> key. A list of users who have not been authorized gateway access will be displayed. Move the cursor up or down until the user you want to add is highlighted and press the <Enter> key. This may be done for as many users as necessary. When you have finished, press the <Escape> key to exit the installation process. If, at a later time, you wish to authorize additional users, you can run INSTAPPS directly from the SYS:\NASIAPPS directory and select the Modify Product Users option when the window is displayed.

   Note: Each copy of ANYWARE and ASCOMIV is licensed and, by way of internal control, allows four concurrent sessions of each product. Consequently, each copy has its

own serial number. If more that four concurrent sessions of either product are required, additional copies of the product must be purchased and installed. To install additional copies of ANYWARE or ASCOMIV, use the following procedure:

- From the SYS:\NASIAPPS directory, key in INSTAPPS and select Install Product.
- Install the product diskette in the disk drive per the instructions.
- At this time, a message similar to "Serial number added" will be received. Afterwards a prompt to re-install the product will be received. Be sure to answer NO to the re-install prompt. If you answer YES, you will write over any script files or batch files you may have previously created.

The procedure for installing additional copies of ANYWARE or ASCOMIV is not provided in any of the manuals. These procedures were obtained directly from NOVELL Technical Support.

Modify/Create Script Files

After all of the software is loaded on the file server and all necessary users have been configured to allow access to the gateway, the Script files must be modified or created for use by the LAN workstations when the gateway is called. These Script files simplify operation of the gateway for users who are not technically oriented. The Script files control all aspects of the gateway session which would otherwise be performed manually. Many script files have been developed for use on the NDPD file servers. These files have been placed on the LANBBS for distribution to all Lan Administrators. Download and use these files, either with or without modification, at your site. If you have any questions concerning these files, contact LANSYS.

OPERATION

Daily operation of the NACS gateway should be divided into two sections; actual gateway operation and use of the gateway by LAN workstations.

Gateway Operation

Daily operation of the gateway requires little effort from those responsible for the gateway. Once the gateway is up and operational, no intervention is required by the LAN Administrator. The only time intervention may be required is if the gateway must be rebooted, such as after a power failure. If the autoexec.bat file is set up correctly, however, the gateway could reboot itself and automatically start the NACS program without LAN Administrator intervention.

Gateway Operation by LAN Workstations

Daily use of the gateway by LAN workstations is simplified by two batch files provided with the gateway software. In the ASCOMIV directory, batch file A4.BAT invokes the loading of the NASI interface software, checks for user authorization for use of the gateway, and calls the ASCOMIV program. In the ANYWARE directory, the batch file AW.BAT performs the same functions.

Note: The NASI interface program used by the NACS gateway is a TSR program that uses 40k of memory. This program does not need to remain TSR for normal gateway use. Use of a mark and release program before loading and after use will unload the program from memory.

This poses another possible problem, however. When you use mark/release to unload NASI, a "file handle" is taken away from the total files available to DOS. When all file handles are used, the workstation receives a "no file handles" error and may hang. The only way to avoid this error is to increase the "files=" parameter in the config.sys file. Increase the count by the number of times you expect to use the NACS gateway between reboots of your workstation PC.

TROUBLE-SHOOTING

Troubleshooting depends on how the ports on your gateway are configured. The most common problem with ports that are connected to modems is caused by a noisy phone line. Unfortunately, the only way to correct this problem is to hang up and redial. In any case, it is advisable to check all connections for a port when a problem is discovered with the port. First, ensure that all cable connections on the gateway end and on the service end are secure.

If the port is connected to a data switch and no response is received from the switch, have someone familiar with the switch check the switch port to ensure that it is working properly. In any case, troubleshooting an ASCII gateway problem requires expertise in ASCII communications as well as certain testing equipment (breakout box or line monitor).

If all connections have been tested and no problems are found, the port on the gateway may be bad. Swap the cable from the gateway to the switch with another on the gateway that is working properly. If the known good gateway port works with the suspected bad switch port, the port on the gateway is probably defective. The WNIM board in the gateway will have to be repaired or replaced if one of the four ports on the board becomes defective.

2. SNA WORKSTATION SOFTWARE

OVERVIEW

The most popular mainframe terminal is the full-screen 3270 series from IBM. The 3270 terminals are used in on-line, interactive sessions with an IBM-type host computer. The Agency mainframe host is an IBM 3090, and the distributed hosts are IBM 4381 processors. The most efficient terminal access to these systems is the 3270 full-screen, synchronous terminals. This service is provided to network users via the 3270 System Network Architecture (SNA) communications gateway. Through emulation hardware and software, a workstation on the network can perform the same functions as the 3270 terminal. Additionally, the network workstation can receive and store files from the host computer, modify or reformat display data, run local application programs, and send output to the host computer.

Emulation software allows the network workstation to perform as a 3270 Type 1 terminal. The 3270 Model 2 display is compatible with the normal PC display, with 24 lines of 80 characters each. The 3270 Model 3 has a 32-line display; the Model 4, a 43-line display; and the Model 5, a 27-line by 132 column display. Workstation software can be configured to allow PC's with Enhanced Graphics Adapter (EGA) and Video Graphics Array (VGA) to emulate true Model 3 and Model 4 displays without scrolling. The workstation emulation program still provides PC's without EGA and VGA with the capability of scrolling via cursor control keys. EPA recommends that workstations be configured as IBM 3270 Model 2 terminals, although EGA and VGA monitors are capable of handling the screen capacities of Model 3 and Model 4 terminals.

Workstations on the LAN can initiate a 3270 session with the mainframe through the gateway. To start the session, the workstation simply loads the emulation software. No special hardware is required at the workstation; the hardware resides in the 3270 gateway server attached to the network.

The workstation software, NetWare 3270 LAN Workstation, provides access to mainframe applications and files through 3270 terminal emulation. (A typical workstation configuration consists of one host session and one DOS session.) In addition, the workstation software supports up to five host display/print sessions at

one time. The file transfer utility is included with the workstation software, permitting users to upload and download data between the PC and the mainframe.

Keyboard functions identical to those of a 3270 terminal are provided on network workstations. The gateway software includes keyboard template overlays, which facilitate function key usage. Manual and utility software is included for remapping the keyboard setup.

One advantage of the Novell gateway is that as many as five simultaneous mainframe sessions can be active on a single workstation. Depending upon the user profiles, each session may take up the entire screen or be displayed in concurrent windows, and users can switch from one session to another.

Advantages of 3270 Workstations

Numerous advantages exist for attaching a networked computer as a mainframe 3270 workstation. A few of these advantages are:

1. The ability to switch back and forth between PC application software on LAN and mainframe sessions.

2. The ability to capture a complete mainframe session for later review or analysis.

3. The ability to extract mainframe information and manipulate it locally on the LAN workstation. Small computational work is downloaded to the local level, reducing the workload on the mainframe.

4. The ability to manipulate downloaded mainframe data with personal computer application programs. Not only does this reduce mainframe costs and resources, but PC applications are typically easier to use and are often more sophisticated for specific applications.

5. The ability to support Novell, IBM, and DCA Application Program Interfaces (API's).

6. The workstation's memory can be used more effectively. NetWare 3270 LAN workstation software requires only 114KB. Added functionality increases memory incrementally, permitting more effective customization.

7. The workstation software can be removed from resident memory, allowing the workstation to run other applications.

INSTALLATION

Software Installation

The current workstation package is called Novell's NetWare 3270 LAN Workstation. Each workstation package contains four 3.5-inch and five 5.25-inch diskettes. Located on the disk titled "NetWare 3270 LAN Workstation Control Program Files" are two files called read.me and readme.ws. The read.me file contains a list and a brief description of the files included on the disks. The readme.ws file contains important information that should be read before installing the workstation software.

To begin installation procedures, the LAN Administrator will log on the file server where the workstation software is to be installed and make a directory (i.e., SYS:APPS\WORKSTAT). The Administrator will then copy the appropriate files to the newly created directory. The files that are needed are located on the 3270 LAN Workstation Control Program Files and the 3270 LAN Workstation Supplemental Control Program Files diskettes.

Four manuals are included with the workstation software package: 3270 LAN Workstation Installation Guide, Workstation User's Guide, Send-Receive User's Guide, and 3270 Keyboard Definition Utility Guide.

After the files have been copied, the Workstation Control Program must be customized. The NetWare Workstation Control Programs are much easier to configure than the Network Server Control Program. Hardware interface customization is not required, as all of these are controlled by the Network Server Control Program. Instead, a Workstation Customization panel is used to define the workstation-to-server connectivity. Workstations can be customized for a PC session, with one to five host sessions. Host sessions can be 3278/79 display sessions (LU Type 2) or 3287 printer sessions (LU Type 1). Details of customizing the Network Workstation

Control Program can be found starting on Page 6 of the Workstation Installation Guide.

Following is an overview of the functions of the installation procedure.

1. Enter the command GWCONFIG WSLAN; where WSLAN designates the name of the Control Program to be customized. A copyright screen will indicate the version of the program running, and prompt for a "YES" to continue.

2. Enter "YES" and the next screen will display the hardware customization panel.

3. Additional screens for various functions relating to the network file server, gateway server, communications link, and host configuration will be displayed. Each of these requires parameters which should be specified according to the particular configuration.

Figure 2-1, Workstation Customization Panels, lists the display panels and parameters that are necessary to complete a single workstation customization procedure; other workstation customizations are similar.

Remote Print Device Setup

Before you can use the workstation control program for remote printing, you must submit a Telecommunications Service Request (TSR) and define the Logical Unit (LU) to be used for a print session, customizing the gateway software with a unique access code. The workstation control program can then be customized to access the LU that is identified at the gateway.

The same procedures used for customizing the workstation control program for a display session can be used for a printer session. These are included in the NetWare 3270 LAN Workstation Installation Guide and can be used for customizing the workstation control program. On page 28 of the manual, an explanation is given of the print options. The Workstation access code must match the access code from the server pool (previously set up at the gateway) that has been defined for the print session. The workstation will then be able to load the emulation program for controlling the print session.

Parameters	Settings	Comments
• **Connection to the Host: LAN Workstation**		
Do you wish to Continue	Yes	
• **Workstation Customization**		
Network Interface to be used	SPX	
SPX Interface Interrupt Number	122	Per Novell
Up to 4 Server Codes:	XXXXXXXX	(net)
	XXXXXXXXXXXX	(node)
(net = Backbone address of Ring where the Gateway is attached)		
(node = Locally Administered Address of Gateway Server)		
Access Code - Server Local Device Pool	WS1	Per Gateway
SPX Receive Buffers for Control Program	6	Per Novell
• **PC Display/Printer Customization**		
Model 3 Font for EGA and/or VGA	no	if desired
Model 4 Font for EGA and/or VGA	no	if desired
Model 5 Font for EGA and/or VGA	no	if desired
Where Printing is to be Directed	LAN printer	
Which Printer to use for Screen Prints	lpt1	
• **Control Unit Option Customization**		
APPC (LU 6.2) Support is Desired	no	
• **General Session Customization**		
PC Session is Desired	yes	
Number of Host Sessions Desired	one	Max 5
Color Adapter Mapping for Host Sessions	Base Color Mode	
• **Host Session 1 Customization**		
Type of Device for this Session	Display	
Host Session Name:	A	
Session Screen Size	Model 2 (24x80)	
Level of Extended Data Stream Support	Extended Attributes	
• **Control Program Option Customization (1)**		
Application Program Interface	111	Per Novell
• **Control Program Option Customization (2)**		
Graphics Adapter 4k Pages to be Saved	One	Max 4
Video Snow Suppression is Required	No	
• **Keyboard Customization**		
Size of Keyboard to be Used	Enhanced	
Keyboard to be Used with Host Sessions	Typewriter	
• **Character Translation Customization**		
Source of National/Keyboard Tables	Predefined list	
Language for National/Keyboard Set	U.S. English	

Figure 2-1. Workstation Customization Panels

The workstation control program can be used to establish a print session to a printer attached to the workstation or use the CAPTURE command to send the print to a shared LAN printer.[1]

Once the workstation has been customized for a remote print session, it can be loaded and unloaded just like a workstation display session. See Page 5-1 of the NetWare 3270 Workstation User's Guide included with the workstation package for correct procedures to activate and control the remote print device.

Batch File Creation

After successful completion and testing of the workstation control program, a batch file should be created. The batch file will map you to the directory where the workstation software resides and execute the emulation program that is desired. An example of the batch file, which is placed in the public directory, is shown in Figure 2-2, SNA Batch File Example.

```
echo off
MAP N:=SYS:APPS\WORKSTAT
N:
WSLAN
HOME
MAP DEL N:
echo on
```

Figure 2-2. SNA Batch File Example

Another batch file example and associated files reside in the INSTALL directory of the LAN Bulletin Board System (LANBBS). This file is archived and should be unpacked before you try to use it. Included with this file is an example of a batch file, a screen detect program to check the monitor type, and a keyboard type prompt program for 83 and 101 key keyboards. Using this

[1] Sending host print to a LAN printer may cause the print to be intermixed with other print. The timeout value should be increased in the CAPTURE command if a problem occurs.

program will allow you to set up one batch file that will handle many different adapter and keyboard types.

File Transfer Installation

Before any file transfers can be performed, the **send.exe** and **receive.exe** files must be copied into the public directory.[2]

The **send.exe** and the **receive.exe** files are located on the 3270 Workstation Send-Receive diskette that is included with the workstation package. Novell includes a NetWare 3270 Send-Receive User's Manual with the workstation package.

Loading and Unloading the Control Program

The **wsexit.exe** program which is located on the NetWare 3270 LAN Workstation Control Program Files diskette is used to unload the emulation program from memory. The **wsexit.exe** should be placed in the public directory. When the emulation software is no longer needed, you simply issue the unload command from the DOS command line or the AUTOMAXX menu.

OPERATION

After the workstation control programs have been customized and copied into the correct directory, very little maintenance is required. Initially, the LAN Administrator will spend most of his time showing users the functionality of the 3270 emulation program.

Accessing and Using the Emulation Program

When you need 3270 terminal access, you must first log onto the file server. Once properly logged, you will be able to call the workstation control program from the DOS command line or AUTOMAXX menu. After the emulation program has been loaded into memory, the workstation will be able to "hot-key" jump between the DOS session and the host session. A template is included with the workstation software that defines the PF keys.

[2] Novell currently has a file, send.exe, for their message handling system. A different name for the file transfer send.exe should be created (i.e., send.exe renamed sendfile.exe).

3179G Graphic Terminal Emulation

3179G graphic terminal emulation can be obtain with the purchase of an additional software package, NetWare 3270 Vector Graphics. The 3179G graphic emulation requires an EGA or VGA monitor adapter and is used in conjunction with the NetWare 3270 LAN workstation software.

The LAN workstation software that's customized for vector graphics must be loaded first. After the workstation control program has been loaded, the vector graphic control program can be loaded. The graphic portion will use approximately 200K of memory.

Once loaded, the vector graphic portion will emulate a 3179G terminal. A template is included to define the function keys and a user's manual, NetWare 3270 Vector Graphics Option User's Guide, is also included.

The vector graphic control program can be unloaded when it is no longer needed without loosing the connection to the host.

Send-Receive Commands

The software supplied by Novell (**send.exe** and **receive.exe**) to perform micro-to-mainframe file transfers has been placed in the public directory and these files can be called from the DOS command line.

To perform a file transfer to the host, you must first sign on to the file server where the workstation software has been placed. To perform the file transfer command, the emulation program must be loaded. This can be performed by calling the batch file from the DOS command or AUTOMAXX menu. The workstation can then hot-key to the host session and sign on. After signing on to TSO and receiving the "ready" prompt, you can hot-key back to your DOS session to perform the file transfer.

Novell has included a manual, NetWare 3270 Send-Receive User's Guide, that lists the correct file transfer format and parameters. Figure 2-3, File Transfer Examples, provides examples for sending and receiving a text file to the host.

```
F:\USER\DBEST\sendfile c:\test.txt 'dxfjsyt.lst(ex1)' ascii crlf
F:\USER\DBEST\receive  c:\test.txt 'dxfjsyt.lst(ex2)' ascii crlf
```

Figure 2-3. File Transfer Examples

Unloading the Control Program

After logging off from the host, the workstation control program can be removed from memory. This will allow software applications that need a lot of memory to run. With the unload program (i.e., WSEXIT) residing in the public directory, it can be called from the DOS prompt or from a selection on the AUTOMAXX menu.

3. SNA GATEWAY

OVERVIEW

The SNA gateway is a Personal Computer that is normally placed on a backbone and allows micro-to-mainframe access. Placing the SNA gateway on the backbone will allow the LAN's bridged to the backbone access to the gateway.

After the SNA gateway software has been customized and loaded, the gateway control program will use most of the memory in the PC. Although the PC runs in non-dedicated mode, it is recommended that the gateway PC be used as a dedicated PC. If the gateway PC is rebooted or powered off for any reason, the workstations that have a session to the host will be disconnected. In the event of a host stop or an Initial Program Loader (IPL), the gateway will automatically reestablish the connection to the host. Some gateways can be configured with up to 128 sessions and 97 workstations connected at one time. To accommodate more users, multiple gateways can be installed on the backbone as necessary.

The SNA gateway can be configured in three different ways: COAX connection, Remote/Synchronous Data Link Control (SDLC) connection, and the Token-Ring Interface Coupler (TIC) connection. Only two of the configurations are discussed here: the Remote/-SDLC connection and the SNA TIC connection. The Remote/SDLC is a synchronous connection to a 37xx communications processor that allows up to 16 host terminal/printer sessions and operates at speeds of up to 19.2 Kbps. Besides the gateway software and token-ring adapter card, the Remote/SDLC connection requires a synchronous adapter and modem.

The SNA TIC connection can allow up to 128 host terminal/printer sessions and as many as 97 workstations on a token-ring network. The host connection is made using a TIC residing in a 3174 terminal control or 37xx front-end processor (FEP).

Access to the SNA gateway is obtained by using the workstation software, which should reside on the file server. Batch files are used to load the workstation control program from the DOS command line or from the AUTOMAXX menu. After the workstation software has been loaded, the PC can emulate a 3270 terminal and hot-key between the DOS and host terminal session.

The gateway and workstation software can be customized to perform various functions, such as:

- Provide Model 2, 3, 4, or 5 type displays.
- Allow multiple sessions (maximum of 5) from one workstation.
- Perform micro-to-mainframe file transfers.
- Set up a remote printer session (RJE).
- Perform host print screens to a local or LAN printer.

INSTALLATION

Host Requirements

The configuration which allows access to the mainframe is dependent on local needs and associated hardware. The presence and number of host print sessions, the number of concurrent sessions to be active per workstation, the total number of sessions available with the gateway, and the number of concurrent workstation users determine each configuration. Currently, the typical EPA configuration for the SNA gateway is sixty-four sessions (for performance reasons), each of which has a mainframe host session with local DOS print session. The planning activity includes the preparation of a TSR for the gateway. This must be done by the LAN designers/planners. The TSR must be submitted with the LAN Plan so the proper interfaces will be available when the LAN is installed. Telecommunications will use the TSR to GEN the major node, which will be used by the SNA gateway to communicate to the host.

Software Installation and Configuration

The Novell NetWare software is distributed with two sets of diskettes. Currently, each gateway contains a set of five 3.5-inch and five 5.25-inch disks. The five disks in each set are labeled Control Program Files, Control Program Files and Miscellaneous Files, 3270 Board Diagnostics, SNA Gateway Status Utility Files, and SNA Gateway Diagnostic Utilities. Some important installation notes are included in a file called readme.ins and a complete list of files and a short description of each are included in the file readme.gw. Both the readme.ins and the readme.gw files are

located on the diskette called "NetWare SNA Gateway Control Program Files". The installer should verify the contents of each of the diskettes by checking the files listed in the documentation against the files on the diskettes.[3]

Configuring the Communication Server

The SNA gateway software can be copied onto the file server or to a floppy disk for configuration and execution. It is not necessary to sign onto the file server or be attached to it in order to bring up the SNA gateway.

The LAN Administrator should make a backup copy of the gateway software and the configuration. When installing the SNA gateway software, the Administrator should make a directory on the file server (i.e., SYS:APPS\SNA) and copy the appropriate files from the Control Program Files and the Control Program Files and Miscellaneous File diskettes. Details for customizing the Control Program are in Novell's Quick Start Guide and in the SNA Administrator's Guide. Both manuals are included with the NetWare SNA gateway package.

INSTALLATION PROCEDURE

- Enter the command GWCONFIG GWSERVER; where GWSERVER designates the name of the Control Program to be customized.

- Additional screens for various functions relating to the network file server, gateway server, communications link, and host configuration will be displayed. Each of these requires parameters which should be specified according to the particular configuration.

- Some of the customizing screens will indicate choices that depend on the settings for the host connection. For example, the SDLC encoding, normally NRZ,

[3] Because the gateway can be one of three configurations (SDLC/Remote, TIC, or COAX), many of the files on the disks will not be needed. See the short description listed in the readme.gw file.

depends on the configuration of the 3705/3725 port. Figure 3.1, Gateway Customization Panel for SDLC Connection, provides relevant information for various screen panels and lists EPA recommended settings.

Parameters	Settings	Comments
o **Host Attachment Customization**		
Type of Connection to the host	Remote	
Remote Board is Synchronous/HS	NO	
o **Hardware Customization**		
Interrupt Level for Interface Board	2	If TRN is 3
SDLC Encoding	NRZ	Per Telecom
o **SDLC Control Unit Option Customization**		
Error Conditions Return an Op Check	Neither	For RJE prt
SDLC Control Unit Address	01	
SDLC Block ID	017	
PUID for Switched Data Link	00000	
o **Network Server Customization**		
Network Interface to be Used	SPX	
SPX Interface Interrupt Number	122	Per Novell
Total Number of Host Sessions	16	Max 16
SPX Receive Buffers for Control Program	200	Per Novell
Receive Buffers for GW Status Utilities	3	Max 5
o **Local Address Type Definition**		
Local Address Type (2=display, 1=printer)		
Model (for Type 2, the 3270 emulation mode)		
Access Code (maintained by the Customization program)		
o **Local Address Pool Definition**		
Local Address Pool (WS1 is used as an example)	WS1	User def.
Concurrent Workstations for Access code	16	User def.
Session per Workstation	1	User def.

Figure 3-1. Gateway Customization Panel for SDLC Connection

Installing and Testing for Remote/SDLC Connection

The Novell Synchronous Adapter is designed to reside in any slot of an AT-type compatible bus. Current Novell synchronous adapters are self-configuring, require no jumper settings, and conform to existing hardware in the gateway server. The interface card may require an I/O address setting via a DIP switch. Refer to the Novell documentation for appropriate DIP switch settings.

The Novell gateway is supplied with a modem cable. If you are not connecting the board to a modem (DTE device), a null-modem

cable may be necessary to attach to another DTE device. To directly connect to a Logical Mainframe (LMF), an IBM Type A PN # 7837395 (ECOA 39478) cable must be ordered separately.

After the cables have been connected to the appropriate devices, the board installation is complete.

Installing and Testing for TIC Connection

The connection to the host via the Token-Ring Interface Coupler (TIC) can be established without any special hardware. It is necessary to connect the cable from the TIC and the cable from the gateway PC to the same ring. The only hardware component required (besides the TIC and TIC cable) is either an IBM Adapter 2 (for PC bus) or an IBM Adapter A (for a micro channel PC). The IBM adapter cards are the same interface cards used in the workstation nodes.

Installing and Configuring Software for TIC Gateway Connection

The procedures for installing software for a TIC connection are the same as those for installation of the Remote/SDLC. The difference will occur when you customize the gateway server software for a TIC connection. An example of the defaults for the customization are included in Figure 3-2, Gateway Customization Panel for TIC Connection.

Testing SNA Gateway Connection

The arduous preparation of the gateway begins with the planning and development of the TSR and culminates with the testing phase. If the procedures for configuring and loading the hardware and software have been followed, the test procedure will proceed rapidly and without encountering problems. Before attempting to test the gateway, recheck the LAN status. If the gateway is to be installed on a new LAN, it is advisable to begin gateway testing with only the file server, the gateway server, and one workstation. Until the gateway and one workstation have been successfully tested, it is not advisable to configure the remaining workstations.

The first step is to confirm with Telecommunications that the gateway has been configured as specified in the TSR. This should be accomplished in advance of the testing and Telecommunications should be alerted to the gateway testing schedule.

Parameters	Settings	Comments
o **Host Attachment Customization**		
Type of Connection to the host	Token-Ring	
o **Token-Ring Server Option Customization**		
Destination Node (Controller) Address	Gen'd TIC Address	
Error Conditions Return an Op Check	Neither	Per Novell
Token-Ring Service Access Point	04	
Block ID	017	
PUID for Token-Ring Connection	E0001	
o **Network Server Customization**		
Network Interface to be Used	SPX	
SPX Interface Interrupt Number	122	Per Novell
Total Number of Host Sessions	64	Per Gateway
TR Receive Buffers for Control Program	50	Per Novell
SPX Receive Buffers for Control Program	100	Per Novell
Receive Buffers for GW Status Utilities	3	Max 5
o **Local Address Type Definition**		
Local Address Type (2=display, 1=printer)		
Model (for Type 2, the 3270 emulation mode)		
Access Code (maintained by the Customization program)		
o **Local Address Pool Definition**		
Local Address Pool (WS1 is used as an example)	WS1	User def.
Concurrent Workstations for Access code	64	User def.
Session per Workstation	1	Max 5

Figure 3-2. Gateway Customization Panel for TIC Connection

The second step is to configure the software for the gateway server and workstation control programs as discussed earlier. This is followed by loading the software onto the file server or gateway server as indicated.

The particular LAN configuration can have more than one host and one printer session per workstation. Once these factors have been determined and the software configured and loaded, the hardware installation can proceed.[4]

In addition to the token-ring adapter, only one hardware item is installed on the LAN for a remote connection; only the token-ring

[4]Installation must conform to the TSR.

adapter is installed for a TIC configuration. It is recommended that the gateway software be installed and run in a dedicated PC.

When configured, the LAN Administrator assigns an interrupt for the adapter. Usually Interrupt Level 2 is chosen (Interrupt Level 3 is reserved for the token-ring adapter required for the LAN).[5]

You should configure the adapter switches to reflect the interrupt level selected and then install the adapter. Connect the adapter to the modem or to the null-modem to provide the data path to the LMF or IBM 3090 mainframe. This step likewise requires planning and a TSR for proper implementation. A special IBM cable will be required if the installation is directly connected to the LMF without modems. (See Installing and Testing for Remote/SDLC Connection on Page 3-4.)

Telecommunications should be called before loading and executing the gateway software. Telecommunications personnel will verify that the gateway connection has been established and the line is active.

If problems occur, Telecommunications will be able to assist in detecting and correcting the problems. NetView and the NetWare Gateway Status Utility can be used to monitor the line (see Diagnostic Procedures, Page 3-8 for further information), determine the status of the emulated controller, and inform the LAN Administrator when the workstation is being polled. The NetWare SNA gateway thoroughly emulates an IBM 3x74 controller; it must be treated as one. This means that occasionally the line has to be dropped, the controller reset, and, on rare occasions, the power must be turned off. Corresponding actions with the gateway software include having Telecommunications personnel drop and reactivate the line, and having the LAN Administrator reboot the gateway server. Normally, the gateway PC remains up and running, as does the file server. When the gateway has been turned off or rebooted, it must be restarted before any workstations are brought up. When a good line is established, the first workstation's software can be loaded and executed. Assistance may be required to establish the line the first time. Thereafter, this process will be routine and transparent to the workstation users.

[5] Problems were encountered using an Epson PC with IRQ2 when running the gateway software. Therefore, it is recommended that IRQ3 be used for the token-ring adapter.

Following successful mainframe connections with the first workstation, the remaining workstations should be activated to ensure that concurrent operations can be performed.

OPERATION

The NetWare gateway software package is very stable. Once the gateway becomes operational, very little maintenance is required. If a problem is encountered with the software, Novell will release a Program Temporary Fix (PTF). LANSYS will place this PTF on the LAN Bulletin Board System (LANBBS). The LAN Administrator can then download the PTF and follow the installation instructions that are included.

The gateway PC should have a batch file that is called from the AUTOEXEC batch file to reload the gateway control program in case of a power failure.

The host or FEP processors may experience hardware or software problems and may be taken down at any time. The SNA gateway will remain up and operational without any intervention. When the host and FEP are brought back on-line, the gateway will re-establish its connection.

DIAGNOSTIC PROCEDURES

Problems may be encountered while installing the SNA gateway. The manual, NetWare SNA Gateways Diagnostic Supplement, which is included with the SNA gateway package, should be consulted first. This manual can be used to resolve many of the gateway and workstation problems. The manual is divided into four chapters: Common Problems and Solutions, Troubleshooting Flowcharts, Diagnostic Menu and Utilities, and Error Messages.

Common Problems and Solutions

The Common Problem and Solution area of the diagnostic manual is presented in four sections: General, Modem, SPX, and Netbios. Each section contains a general description of the problem and a solution that may help correct the problem.

Most of the sections are not listed in any particular order, so to find the information that relates to a specific problem, it may be necessary to read through all of them.

The Netbios section will not be needed at this time. Currently, all of the Agency gateways are set up to use the Sequenced Packet Exchange (SPX) interface.

Troubleshooting Flowcharts

The Troubleshooting Flowcharts section contains eight flowcharts and provides instructions for identifying and resolving SNA gateway and gateway workstation problems. The Troubleshooting Flowcharts section starts on Page 25 and ends on Page 41.

Diagnostics Menu and Utilities

Chapter three of the diagnostic supplement describes how to install and use the SNA Gateway Diagnostics menu and utilities. The diagnostic menu and utilities can be a valuable troubleshooting tool for isolating problems with the gateway. A brief explanation detailing the utility is included.

Error Messages

Chapter four of the Diagnostic Supplement contains a list of common error messages along with an explanation of each and the corrective action to be taken. The error messages are listed in alphabetical order for quick access.

SNA Gateway Status Utility

The SNA Gateway Status Utility is included with the gateway software on the diskette labeled NetWare SNA Gateway Status Utility Files. The files included are: $run.ovl, gwstatus.exe, gwstatus.hlp, ibm$run.ovl, sys$err.dat, sys$help.dat, and sys$msg.dat. Once the software is installed, it can be called from any workstation attached to the LAN.[6]

Figure 3-3, Gateway Status Utility, is an example of the gateway status utility. To execute the program, simply change to the directory where the gateway status software resides and type GWSTATUS. The program will prompt for a ring address (the ring address is where the gateway PC is attached) and an update interval (time used between status displays).

[6] The number of simultaneous gateway status programs cannot exceed the number specified when customizing the gateway software. The maximum number that can be used is 5. If more workstations are using the gateway status utility than specified, Novel warns that the gateway will crash.

Gateway Status Summary and Session Information

Maximum Sessions:	64	Host Connection Type:	Token Ring
Sessions Active:	7	Host Link Status:	Active
Sessions Inactive:	55	LAN Errors:	1
Sessions with Errors:	0	Memory Utilization (k):	419
Workstations Connected:	10	GW Uptime (hhhh:mm:ss):	0038:23:39

GW/LU	UserID	Internetwork Address	Access Code	Status	Appl ID	LE
2/2	JSMITH	0000008210005A1D5CCB	MAINPOOL	UBOUND	TSO0423	0
2/3				DACTIV		
2/4	BJONES	FFFFFFF410005ACD7789	MAINPOOL	UACTIV		

Figure 3-3. Gateway Status Utility

When the Gateway Status Utility is displayed, addition help keys are available. The PF1 key is used for on-line help and the enter key is used for specified user information. Additional information and definitions can be found in the SNA Gateway Administrator's Guide located in the SNA Gateway Status section.

Remote Print Device

Planning for a remote print session can be included with the initial LAN plan or after the LAN has become operational.

The TSR must include the LU number that will be used for the remote print device. The LU number included with the TSR will be used by systems when performing the GEN.

Changes to the SNA gateway software will not be necessary; however, the workstation software will need to be customized. (See the Workstation Customization section for remote print devices).

4. DIRECTORY STRUCTURE

OVERVIEW

Directory Structure

All network information is stored on the file server's hard disk. The system for storing this information is called the directory structure.

Information is organized logically on the hard disk in units called files. For example, a file might be a letter or a list of addresses. When you save information in a file, you give the file a unique name so you can retrieve it later.

On a NetWare file server's hard disk, files are organized to make them easy to find. The system is broken down as follows:

File servers contain
  Hard disks, which are divided into one or more
    Volumes, which are divided into
      Directories, which are divided into
        Subdirectories, which contain
          Files.

In general, directories can be thought of as having a tree or hierarchical structure; that is, there is a root directory broken down into branch directories, each of which may contain additional subdirectories, and so on. The advantage of this organizational structure is that it allows program and data files for a particular application program to be kept separate from files that belong to a different application. Instead of searching through a long list of files from a variety of applications, you need only change to the appropriate subdirectory and search through its files.

INSTALLATION

Directory Structure

A group of default directories is created when the server is first initialized. The SYSTEM, LOGIN, and PUBLIC directories are created by the Novell operating system. The USER, SUPER, and APPS directories are created by the server set-up routine performed by SMA.

Figure 4-1, illustrates the typical directories which can be found on a file server.

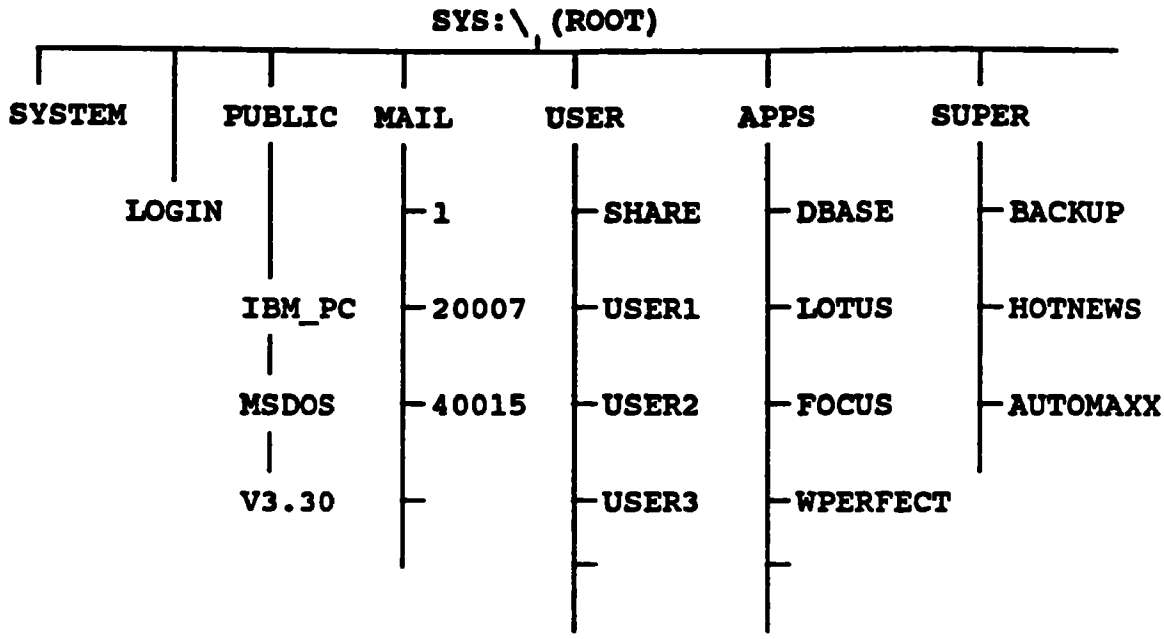


Figure 4-1. Typical Directories on File Server

Directory names and contents:

SYSTEM. Contains the network operating system, along with certain server utilities to which the network Supervisor should be allowed access.

LOGIN. Directory used during the LOGIN and LOGOUT process; contains LOGIN.EXE and SLIST.EXE programs. The LOGIN.EXE file is the program executed when you type "LOGIN" at the workstation. The SLIST.EXE file is the program that lists all servers by name that are currently attached to the network.

MAIL. Has numbered subdirectories that can serve as "mailboxes" (not used at EPA) and store users' login script.

PUBLIC. Contains NetWare utilities and BAT files which a user can execute.

USER. Contains a "HOME" subdirectory for each user and a subdirectory that all users can share.

APPS. Contains applications software programs, such as word processing, spreadsheet, data base, etc.

SUPER. Contains items maintained by the LAN Administrator, such as server files backup, news, and AUTOMAXX menu system.

OPERATIONAL

Directory Structure

To maintain the Agency server directory structure, you should follow DOS directory structure format; that is, the root directory will have /SYSTEM, /LOGIN, and /PUBLIC directories; the /USER directory will have users' HOME directories and a SHARE directory, and the /APPS directory will have application software directories (such as dBASE, LOTUS, WordPerfect, etc.). Using this structure, the appropriate program and data files will be installed in their respective directories, and each user will have his/her own personal directory for private files.

The DOS command function MKDIR can also be used to create new directories, and the RMDIR command can be use to remove directories. If you are proficient in the use of DOS, these commands may be somewhat easier and faster when implementing a directory structure rather than using the FILER program.

1. CREATE DIRECTORY USING DOS MKDIR COMMAND

   The process of creating new directories using DOS MKDIR is as follows:

   - Position yourself at the current directory.
   - At the DOS prompt, type: MKDIR NEW-DIR <Enter>

   The new directory "NEW-DIR" will be created under the current directory.

2. CREATE DIRECTORY USING FILER

The process of creating new directories using FILER is as follows.

- At the DOS prompt, keyin: FILER <Enter>
- Select the "Select Current Directory" option on the FILER main menu.
- A window for typing the new path will be displayed. Use the backspace key to delete the directory information displayed. Type 'SYS:/'. This will ensure that the current directory is the root directory.
- From the FILER main menu, select the "Subdirectory Information" option on the menu
- A list of Subdirectories will be displayed. The directories that were created when the operating system was installed (PUBLIC, MAIL, SYSTEM, and LOGIN) should be displayed.
- Press the <Ins> key. A window for typing the new directory name will be displayed. Repeat this step for each of the directories you wish to create directly from the root directory.
- To create subdirectories, change the current directory to the directory which will contain the subdirectories; then repeat the steps for adding directories as outlined in Steps 4 through 6.
- Press <Esc>, then Exit FILER.

TROUBLE-SHOOTING

Directory Structure

If the Agency file directory structure guidelines are used, there should be no problem in locating or accessing file directories on the network. Any problems experienced could be caused by attempting to access a non-existent directory, entering an incorrect file path,

or attempting to access a directory without having access rights to the directory. The LAN Administrator can check for the existence of the directory or use the SYSCON utility to verify the user's file trustee assignments.

5. LOGIN SCRIPT

OVERVIEW

A login script is a series of NetWare commands executed automatically when a user logs into the file server. Two login scripts are associated with every login: System and User.

The System Login Script is a series of NetWare commands applicable to every user who logs into the file server. It is the first script executed when a user logs in. Because it is applicable to every network user, the System Login Script contains the minimal number of NetWare commands necessary for network functioning. The LAN Administrator can modify this default by using the SYSCON utility.

The second login script to be executed when a user logs into the file server is the User Login Script. This script is also a series of NetWare commands. It contains the commands that customize file server access for the network user.

INSTALLATION

A standard EPA System Login Script should be installed on file servers purchased from SMA. It can be modified by the Supervisor or anyone having Supervisor rights. Care must be taken when modifying Script since several other system functions may be affected. If unsure of the impact that your modifications may have, contact LANSYS for assistance. Each user can modify his/her own login script by using the SYSCON utility.

If appropriate login script commands have been entered and many convenient tasks will be performed automatically for you when you log in.

Modifying the System Login Script

Following are steps for modifying the System Login Script:

1. At the DOS prompt, type : SYSCON <Enter>

   The SYSCON "Available Topics" menu will be displayed.

2. Highlight **Supervisor Options** and press <Enter>. The "Supervisor Options" menu will be displayed.

3. Highlight **System Login Script** and press <Enter>. The System Login Script will be displayed.

   You can use any of the commands explained in Appendix A of the Supervisor Reference Manual to modify a System Login Script.

4. To exit the System Login Script, press <Escape>. (If you have changed the login script, you will be asked to confirm that you want to save the changes before you exit.)

Figure 5-1 is an example of the Default System Login Script.

```
* SYSTEM LOGIN SCRIPT
MAP DISPLAY OFF
* MAP SEARCH DRIVE "Z" TO \PUBLIC
MAP S16:=SYS:PUBLIC
* MAP A SEARCH PATH (DRIVE "Y") FOR DOS 3.30 USERS ONLY
IF "%OS_VERSION"="V3.30" THEN BEGIN
MAP S16:=SYS:PUBLIC\%MACHINE\%OS\%OS_VERSION
END
* MAP DRIVE G: TO THE \USER\SHARE DIRECTORY
MAP G:=SYS:\USER\SHARE
* DRIVE F: = USER'S HOME DIRECTORY
IF "%LOGIN_NAME" IS NOT "SUPERVISOR" THEN MAP
   F:=SYS:\USER\%LOGIN_NAME
* GREET THE USER
WRITE "Good %GREETING_TIME, %FULL_NAME"
* F: = DEFAULT DRIVE UPON LOGIN
DRIVE F:
* SET DOS PROMPT TO DISPLAY DEFAULT DRIVE AND DIRECTORY
SET PROMPT="$p$g"
* SET ENVIRONMENT FLAG USERID TO LOGIN NAME FOR MENU SYSTEM
DOS SET USERID="%LOGIN_NAME"
IF "%LOGIN_NAME" IS "SUPERVISOR" THEN DOS SET USERID="SUPER"
MAP DISPLAY ON
* SHOW THE USER WHAT HAS BEEN MAPPED
MAP
* DISPLAY "HOT" NEWS
DISPLAY SYS:SUPER\HOTNEWS\HOTNEWS
IF "%LOGIN_NAME" IS NOT "SUPERVISOR" THEN  PAUSE
```

Figure 5-1. Example of EPA Default System Login Script

Creating or Modifying User Login Script

Following are steps for modifying the User Login Script:

1. At the DOS prompt, type : SYSCON <Enter>
   The "Available Topics" menu will be displayed.

2. Highlight User Information and press <Enter>.

3. Highlight the user you want to assign a login script to and press <Enter>. The "User Information" menu will be displayed.

4. Highlight Login Script and press <Enter>. The "Login Script Does Not Exist" box will appear.

5. Use the Backspace key to delete the user name listed. Type in the name of the user whose Login Script you want to create and press <Enter>.

   A blank screen of Login Script For User <Username> will be displayed. You can enter the Login Script commands for this user.

   Example of EPA default User Login Script:

   EXIT "MENU"

6. To exit the User Login Script, press <Escape>. (If you have changed the login script, you will be asked to confirm that you want to save the changes before you exit.)

OPERATIONAL

The LAN Administrator can use the SYSCON utility to modify System and User Login Script. And, each user, once logged into the file server, can modify his/her own Login Script. Care should be taken when modifying the System Login Script because this script will be executed for every user logging onto the server.

Login Script Commands

You can use the following Login Script commands to customize your login script:

ATTACH
BREAK

COMSPEC
DISPLAY AND FDISPLAY
DOS BREAK
DOS SET
DOS VERIFY
DRIVE
EXIT
EXTERNAL PROGRAM EXECUTION (#)
FIRE PHASERS
IF ... THEN
INCLUDE
MACHINE NAME
MAP
PAUSE
PCCOMPATIBLE
REMARK
WRITE

Each of the Login Script commands is explained in Appendix A of the Supervisor Reference Manual.

Note: When you enter Login Script commands, be sure to end each line by pressing the <Enter> key. Words that are wrapped automatically onto the next line (because the end of the line was reached) are still considered part of the previous command.

Only a few restrictions apply:

- Command lines cannot exceed 150 characters. To increase readability, however, we recommend that you use only 78 characters per line--the width of your screen.

- Only one command can be entered on each line.

The SYSCON utility has a self-contained screen editor and a Help system that you can use to edit your Login Script. Press the Help key at any time during editing to receive help.

TROUBLE-SHOOTING

Incorrect usage of Login Script commands could caused problems or disallow users access to the file server. Check Appendix A of the Supervisor Reference Manual for proper usage of Login Script commands. The Login Script error messages are also described in the NetWare System Messages Manual. Use the SYSCON utility to access the Login Script and correct the errors.

6. USER CONFIGURATION

OVERVIEW

Before a user can access the file server he/she must be given an identification and access rights to the file directories on the server. Each user on the server will be given a login name using the EPA naming convention (first character of the first name and up to seven characters of the last name) and a default password (can be changed with the Novell SETPASS command or through SYSCON utility). Each user will be assigned to a common group (EVERY-ONE). This group has limited rights to most directories on the server such as: /PUBLIC (NetWare utilities), /LOGIN (login program), and /APPS (applications software). Users will have a working area on the file server in which to store their data or programs. This area is called the HOME directory, which is a subdirectory of the /USER directory. Users will have all access rights to their HOME directories and users will be given appropriate security for their work.

INSTALLATION

The Novell operating system automatically creates the Supervisor. The Supervisor is permanent, and has all rights in all servers and file directories.

As a Supervisor, you can use the SYSCON utility to create and configure new users on the server.

The following steps show you how to configure a user on the file server using the SYSCON utility:

1. To access the SYSCON utility, at DOS prompt, type

   SYSCON <Enter>

   The "Available Topics" menu will appear.

2. Highlight User Information and press <Enter>.

3. Press <Insert>. In the "User Name" entry box, type

   JDOE <Enter>

JDOE will now appear on the "User Names" list.

4. With the highlight bar on JDOE, press <Enter> to move to the "User Information" menu.

   Highlight **Full Name** and press <Enter>, then type

   John Doe <Enter>

5. Highlight **Change Password** and press <Enter>. The "Enter New Password" box will be displayed. Type the password in the box.

6. Confirm the new password by retyping it in the "Retype New Password" box. Press <Enter>.

7. Highlight the **Groups Belonged To** option and press <Enter>. The "Groups Belonged To" box will list all groups that JDOE belongs to. (Every user is automatically assigned to group EVERYONE.)

8. To make JDOE a member of another group, press <Insert>. A list of groups that JDOE does not belong to will appear.

9. With the selection bar on "other group", press <Enter>. JDOE now belongs to group "other group".

   Press <Esc>, to return to the "User Information" menu.

10. Highlight **Trustee Assignments** and press <Enter>. The user's trustee assignments will be displayed.

11. Press <Insert>. The "Directory In Which Trustee Should be Added" entry box will be displayed.

12. Specify the directory in which you want to make the user a trustee.

    If you know the directory name, type it and press <Enter>.

    If you specify a nonexistent directory, you will be asked if you want to create that directory.

If you do not know the directory name, press the <Insert> key to list the available file servers. Highlight the file server you want to access and press <Enter>.

In the "Available Volumes" list, highlight the volume you want to access and press <Enter>.

In the "Network Directories" list, highlight the directory you want and press <Enter>.

Continue choosing directories until you have specified the full directory name. Then press <Escape> and <Enter> to make the user a trustee of the directory you have specified.

13. The directory will be listed in the "Trustee Assignments" window with [ROS] rights. To grant additional rights for this user to the directory, highlight the directory and press <Enter>. Press <Ins> and the "Trustee Rights Not Granted" window will be displayed. Use <F5> (Mark key) to select the additional rights, then press <Enter>. Press <Esc> and the additional rights will be added to that directory.

14. Press <Esc>, and Exit SYSCON.

For more information on the SYSCON utility, refer to the NetWare Menu Utilities Manual, Chapter 2.

OPERATIONAL

Once a user has been configured, maintenance of the user configuration is minimum. The LAN Administrator can use the SYSCON utility to reset the user's password, add or delete users to a group, and grant or revoke trustee rights to a file directory.

RESET PASSWORD

Unless you are a Supervisor or have Supervisor equivalence, you can change only your own password.

To change a user's password, follow these steps:

1. At the DOS prompt, type SYSCON <Enter>

2. Highlight Change Password in the "User Information" menu and press <Enter>. The "Enter Old Password" entry box will be displayed. If you did not have a password previously, the "Enter Old Password" box will not be displayed.

3. Type in your old password and press <Enter>. The "Enter New Password" entry box will be displayed.

4. Type in your new password and press <ENTER>. The "Retype New Password" entry box will be displayed.

5. Retype your password and press <Enter>.

Adding User to a Group

To add a user to an existing group, follow these steps:

1. At the DOS prompt, type : SYSCON <Enter>. The "Available Topics" menu will be displayed.

2. Highlight User Information and press <Enter>. The users on the current file server will be displayed.

3. Highlight the user you want to add to a group and press <Enter>. The "User Information" menu will be displayed.

4. Highlight "Groups Belonged To" and press <Enter>.

5. Press <Insert> to see a list of groups the user does not belong to. The "Groups Not Belonged To" entry box will be displayed.

6. Highlight the group to which you wish to add the user. If you want to add the user to more than one group, use the Mark key (F5) to mark each group. Press <Enter>.

   The user is now a member of the selected group.

Deleting a User from a Group

To delete a user from a group, follow these steps:

1. At the DOS prompt, type: SYSCON <Enter>. The "Available Topics" menu will be displayed.
2. Highlight User Information and press <Enter>. The users on the current file server will be displayed.
3. Highlight the user you want to delete from a group and press <Enter>. The "User Information" menu will be displayed.
4. Highlight "Groups Belonged To" and press <Enter>.
5. Highlight the group from which you want to delete the user. If you want to delete the user from more than one group, use the Mark key (F5) to mark the additional groups. Then press <Delete>.
6. In the "Delete User From Group" confirmation box, highlight Yes" and press <Enter>.

   The user has now been deleted from the group.

Making a User a Trustee of a Directory

To make a user a trustee of a directory, follow these steps:

1. At the DOS prompt, type : SYSCON <Enter>. The "Available Topics" menu will be displayed.
2. Highlight User Information and press <Enter>. The users on the current file server will be displayed.
3. Highlight the user you want to make a trustee of a directory and press <Enter>. The "User Information" menu will be displayed.
4. Highlight Trustee Assignments and press <Enter>. The user's trustee assignments will be displayed.

5. Press <Insert>. The "Directory In Which Trustee Should be Added" entry box will be displayed.

6. Specify the directory in which you want to make the user a trustee.

   If you know the directory name, type it and press <Enter>.

   If you specify a nonexistent directory, you will be asked if you want to create that directory.

   If you do not know the directory name, press the <Insert> key to list available file servers. Highlight the file server you want to access and press <Enter>.

   In the "Available Volumes" list, highlight the volume you want to access and press <Enter>.

   In the "Network Directories" list, highlight the directory you want and press <Enter>.

   Continue choosing directories until you have specified the full directory name. Then press <Escape> and <Enter> to make the user a trustee of the directory you have specified.

   The user now has all trustee rights in the specified directory.

7. Now you can add or delete the user's trustee rights in the directory.

   Press <Enter>. The "Trustee Rights Granted" list will be displayed.

   - DELETING: To delete a given trustee right, highlight that right. If you want to delete several rights, use the Mark key to mark them. Press <Delete>.

     In the "Revoke Trustee Rights" confirmation box, highlight Yes and press <Enter>. The right has been revoked.

- ADDING: To add a given trustee right, press <Insert>. In the "Trustee Rights Not Granted" list, highlight the right you want to add. If you want to add several rights, use the Mark key to mark them. Press <Enter>. The right has been granted.

TROUBLE-SHOOTING

The LAN Administrator can use the SYSCON utility to maintain a user's configuration on the file server and check file directory trustee rights for a user. The Supervisor can reset a user's password, add or delete users to a group, grant or revoke trustee rights to a file directory, or delete a user from the server.

7. PRINTING

OVERVIEW

Networks allow a number of people to share the same printer since network printers are connected either to a file server or to a workstation. If the printer is connected to a workstation, a product called LANSPOOL (Section 12) must be installed. When you print on a network printer, you do not send print job requests directly to the printer. Instead, you send your requests to the file server. There they wait in line in a print queue, along with other users' print job requests, until the printer can service them. Print job requests are stored and serviced in the order in which they are received.

To use the network printer, the NPRINT or CAPTURE commands must be executed. The NPRINT command directs print to the network printers. The CAPTURE command tells NetWare to intercept any print job and send it to the network printer spooler before sending it to the printer. Some applications (for example: WordPerfect Network Version) are designed for use on a network. Users can print their output directly within the application to network printers without using NPRINT or CAPTURE commands.

INSTALLATION

To print on the network printers (if your application does not allow you to print directly within the application), you must use the NetWare printing utilities. NPRINT, CAPTURE, and ENDCAP are the NetWare command line utilities used for printing. PCONSOLE, PRINTCON, and PRINTDEF are the NetWare menu utilities used for printing. These utilities are supplied by Novell and resided in the SYS:/PUBLIC directory.

CAPTURE and ENDCAP are the command line utilities that you use to print when you cannot send a file directory to a network printer, either from inside an application or through NPRINT. The NPRINT utility transfers files to the network printer. The files must either be in ASCII format or formatted by the application with the correct control characters for a designated printer. NPRINT uses your default PRINTCON Print Job Configuration when you print a file unless you specify different parameters by using the NPRINT command flags. Before you can use the Print Job Configuration,

the print device functions, modes, and forms must be defined. This can be done with the PRINTDEF utility.

The Network Supervisor can define print device functions, print modes, forms, and print job configurations using PRINTDEF and PRINTCON.

Defining Print Device Functions

To define a printer's functions, complete the following steps:

1. At the DOS prompt, type PRINTDEF and press <Enter>.

2. From the "PRINTDEF Options" menu, choose "Print Devices" and press <Enter>.

3. From the "Print Device Options" menu, choose "Edit Print Devices" and press <Enter>.

4. From the "Defined Print Devices" list, press <Insert>.

5. In the "New Device Name" entry box, type the name of the print device and press <Enter>. The name should be recognizable to users (for example: HP LaserJet).

6. Choose the print device you want to define, and press <Enter>.

7. From the "Edit Device Options" menu, choose "Device Functions" and press <Enter>.

8. In the "Device Functions" list, enter the escape sequences or printer commands for the specified print device. Be sure to include the reset escape sequence.

   To enter a device function, press <Insert>. In the "Function Definition Form" entry box, enter a name to identify the printer command (e.g., Landscape Orientation, Reset, etc.). Press <Enter>.

   The selection bar will move to the "Escape Sequence" option. Enter the actual escape sequence (e.g., <esc>&l1O or <esc>E). Press <Enter>.

Press <Escape> and then <Enter> to insert the new escape sequence into the functions list.

9. Repeat Steps 5 through 8 for each function or escape sequence you want to enter.

10. After you have entered all the device functions, press <Escape> to return to "Edit Device Options" menu.

Defining Print Device Modes

Once you have defined the functions for a print device, you can combine these functions into modes. A mode is a sequence of print functions which tells the printer how to print a particular job. For example, you could create a "Final Print Out" mode that includes the functions for Landscape or Portrait Printing. Determine what your printing needs are, and define the modes accordingly.

To define print device modes, complete the following steps.

1. From the "Edit Device Options" menu, choose "Device Modes" and press <Enter>. The "Reinitialize" mode will appear in the "Printer Device Name Modes" entry box. Press <Enter>.

2. In the "Reinitialize Functions" list, press <Insert> to see a list of all defined modes for one print device. Most devices have a single escape sequence for reset. Choose the function or escape sequence for the reset and press <Enter>.

   If your printer does not have a single reset function, then you will need to enter all your printer's "Cancel" functions into the Reinitialize mode.

   After you have entered the Reinitialize mode functions, you can create your own modes. Each print device has its own set of modes.

3. In the "Printer Device Name Modes" list (Printer Device Name will be replaced by whatever you are defining), press <Insert>.

4. In the "New Mode Name" entry box, type the name of the mode you want to create (e.g., Print Landscape) and press <Enter>.

5. In the "New Mode Name Functions" list, (New Mode Name will be replaced by the name of the mode you are defining) enter the functions for that particular mode. Press <Insert> to see a list of all defined functions for that print device.

   The functions you choose will appear in the "New Mode Name Functions" list. You can edit the functions you choose. If you want to delete a function from the list, choose the option you wish to delete and press <Delete>. To add additional functions to the list, repeat Step 6.

   When you have completed entering and editing the functions list, press <Escape> to return to the "Modes" list.

6. Repeat Steps 4 through 6 for each mode you want to create. When you are finished entering modes for one print device, press <Escape> to return to the "Defined Print Devices" list.

You will need to repeat the "Defined Print Device Functions" and "Defining Print Device Modes" sections for each print device you will be using.

Defining Forms

Print forms are the types of paper on which you wish your output printed. The print forms you define will be used as you set up print job configurations. For example, you might want one job printed on regular 8 1/2 X 11 sheets of paper and another on green bar continuous feed paper.

The file server recognizes forms by name and number. When you send a print request that requires a specific form, the file server will not print the job until that form is mounted on the printer.

To define print forms, complete the following steps:

1. To access the PRINTDEF utility, type PRINTDEF and press <Enter>.

2. Choose "Forms" and press <Enter>.

3. Press <Insert>.

4. In the "Forms Definitions Form" entry box, type the name of the new form you want to define and press <Enter>. The first character of the form name must be alphabetic, and the form name cannot exceed 12 characters.

   Type the number you want to assign to the form and press <Enter>. You will probably want to assign the most commonly used form as form 0, since 0 is the default. Form numbers must fall between 0 and 255.

   Type the length of the form in lines per page and press <Enter>. The number must fall between 1 and 255.

   Type the width of the form in characters per line and press <Enter>. The number must fall between 1 and 999.

5. Press <Escape> and then answer "Yes" to the "Save Changes" confirmation box. Press <Enter>. The new form will be listed in the "Forms" list.

6. Repeat Steps 1 through 5 for each form you want to define.

7. To exit the PRINTDEF utility, press <Escape> twice and then <Enter> to access the "Exit Options" menu. Choose "Save Data Base, then Exit" and press <Enter>.

Print Job Configuration

As a Supervisor, you can create print job configurations for all users, using the forms, devices, and modes defined in PRINTDEF; select the default print job configuration; and copy print job configurations from one user to another.

Users can also set up their own print job configurations. When printing, they can choose this configuration instead of manually entering all the print job specifications. The printer will be returned to its default setting after the job is completed.

Create Print Configuration

You can set up a print job configuration by specifying certain parameters. To do this, complete the following steps:

1. At the DOS prompt, type PRINTCON and press <Enter>.

2. From the "Available Options" menu, select "Edit Print Job Configurations" and press <Enter>.

3. Press <Insert>.

4. Type the name of the print job configuration you wish to add in the "Enter New Name" entry box (e.g., MY-print) and press <Enter>. The "Edit Print Job Configuration" form will be displayed.

   To make changes in the job configuration, choose the item you want to modify and press <Enter>. Then make the appropriate change by typing in a new value or by choosing an item from the menu provided. After you have made the change, press <Enter> to save the change.

5. Once you have set up your job configuration, press <Escape>.

6. Choose "Yes" and press <Enter> to confirm that you wish to save the changes.

Copying Print Job Configurations

Each user has a unique file in which to store his/her print job configurations. As Supervisor, you can copy print job configurations from one user to another. You cannot copy a single job configurations at a time, but must copy the whole file, including all job configurations. If one user's print job configuration file is copied to another, it overwrites the target user's existing file. Since users can create their own print job configurations, you should check with a user before copying another user's file over an existing file.

To copy a print job configuration from one user to another, complete the following steps:

1. At the DOS prompt, type PRINTCON and press <Enter>.

2. From the "Available Options" menu, choose "Supervisor - Copy Print Job Configurations" and press <Enter>.

3. In the "Source User" entry box, type the name of the user whose job configuration file you want to copy and press <Enter>.

4. In the "Target User" entry box, type the name of the user whose print job configuration file you want to place and press <Enter>.

5. Press <Escape> to exit the PRINTCON utility. The second user can now use all of the first user's job configurations.

OPERATIONAL

Although the network handles printing requests differently than standalone personal computers do, it's possible that you will print files as you always have. If you are using an application that is designed to work on a network, you can probably print your files from within the application, just as you would on a standalone personal computer.

If you cannot print to the network printers from within your application, you must use the NetWare printing utilities. These programs are: PCONSOLE, NPRINT, CAPTURE, and ENDCAP.

Using the Printing Menu Utilities

The network supervisor uses PRINTDEF to define modes and forms which are used to set up print job configurations (definitions that tell the printer how to print a document). You set up print job configurations in PRINTCON. PCONSOLE allows you to access a print queue and insert a print job into it. From PCONSOLE, you may specify how you want the job to be printed, choosing from the print job configurations set up by either you or your network supervisor.

If you have not defined any print job configurations, you can use the system default configuration (called PCONSOLE Defaults). Once you specify how you want the job printed, it will wait in the queue until the printer is able to print it.

Printing a File with PCONSOLE

When using PCONSOLE to print the file MY-FILE from SYS:USER/-GUEST directory, follow these steps:

1. At the DOS prompt, type : PCONSOLE <Enter>

2. Highlight **Print Queue Information** in the "Available Options" menu and press <Enter>.

3. Highlight the print queue you want to use in the "Print Queues" list. Press <Enter>. (If you are not sure which print queue to use, ask your network Supervisor.)

4. To see the contents of the queue, highlight **Current Print Job Entries** in the "Print Queue Information" menu and press <Enter>. The jobs waiting to be printed will be displayed.

5. To add a print job entry, press <Insert>. The "Select Directory to Print From" box will be displayed.

6. Use the Backspace key to delete the parts of the directory path that are incorrect. Type the appropriate information so that FILESERVER/SYS:USER/GUEST appears in the "Select Directory to Print From" entry box. (Replace FILESERVER with the name of your file server.) Press <Enter>.

7. Highlight MY-FILE in the "Available Files" list, and press <Enter>.

8. Now that you have specified the file you want to print, you must choose the way you want the file to be printed. Highlight **PConsole Defaults** (the system-created defaults) and press <Enter>.

   The file MY-FILE will be added to the queue. However, you can first modify the print job if you like. The "New Print Job to be Submitted" box allows you to put the print job on hold, change the number of copies to be printed, and change other print job specifications. (These specifications are described in Chapter 7 of the NetWare Menu Utilities Manual.) For example, to change the number of copies that will be copied from 1 to 5, highlight the space after "Number of Copies" and type: 5 <Enter>

9. The file MY-FILE is ready to be submitted to the queue. To do so, press <Escape>.

10. Now press <Enter> to confirm that you want to save the changes you have made. The job will be added to the queue and printed when the printer is available.

11. To exit PCONSOLE, press <Escape> until the "Exit PConsole" confirmation box appears (or press <Alt><F10>). Highlight Yes and press <Enter> to exit to DOS.

Printing a File with NPRINT

You may use NPRINT to print the file MY-FILE, which was saved in ASCII text format when it was created. Because you are at SYS:USER/GUEST and MY-FILE is in that directory, you do not need to specify the directory path when you execute the command (otherwise you will have to specify full path name).

1. At DOS prompt, type: NPRINT MY-FILE <Enter>

2. MY-FILE will be sent to the queue, where it will wait to be printed.

You can specify various flags along with the NPRINT command. You can also specify a form, mode, or job that you have set up in PRINTCON or PRINTDEF. For a complete discussion of the options available with NPRINT, see Chapter 2 of the NetWare Command Line Utilities Manual.

Printing a File using CAPTURE and ENDCAP

CAPTURE and ENDCAP are command line utilities that you use to print when you cannot send a file directly to a network printer, either from inside an application or by using NPRINT.

For example, you can use CAPTURE and ENDCAP to print a workstation screen display. ENDCAP stops the CAPTURE sequence and sends the recorded data to the file or printer you specified in the CAPTURE command.

To print a screen display, you must use CAPTURE and ENDCAP to save the contents of the screen into a file, and then send the file to a Local Printer Port (LPT). In this practice session, you will print a copy of your drive mappings. To do so, you must display your drive mappings on the screen, and then send them as a file to the printer.

1. At the DOS prompt, type: CAPTURE <Enter>

2. Type: MAP <Enter>

   A list of your drive mappings will appear on the screen.

3. Press <Shift> and <PrtSc> simultaneously.

4. Now type: ENDCAP <Enter>

The contents of your workstation screen will be the default printer.

For a complete explanation of CAPTURE and ENDCAP, including instructions on how to print from within a non-networked application, see Chapter 2 of the NetWare Command Line Utilities Manual.

TROUBLE-SHOOTING

Typically, problems experienced with network printers are caused by incorrect NPRINT or CAPTURE parameters, printer off-line, or printer out of paper. An incorrect NPRINT or CAPTURE parameter could cause the operating system to route files to a different printer or not print the job. An off-line printer could be caused by cabling or power problems.

NPRINT and CAPTURE parameters are explained in detail in the Novell Command Line Utilities Manual.

8. SYSCON/FILER/FCONSOLE

INITIAL NETWORK SETUP AND VERIFICATION

Reliability and ease of use are the primary measures of the success of the LAN. Although EPA's standard file servers are shipped with basic menu and directory structures in place, the LAN Administrator must install most applications and all user accounts.

Two NetWare utilities allow the Administrator to establish user accounts: MAKEUSER and SYSCON. The former is a command-line utility which requires the use of ASCII Script files and is most useful when large numbers of accounts must be created at once. It's very powerful, but difficult to use. The latter is a fully interactive, menu-driven program that's relatively simple and has many capabilities beyond those provided by MAKEUSER. For that reason, our discussion is limited to SYSCON.

Directories can be created and deleted using either the NetWare FILER utility or the standard DOS MKDIR/RMDIR commands. FILER is also menu-driven and allows assignment of directory rights to users or groups of users.

The LAN Administrator must become familiar with all aspects of both the FILER and the SYSCON utilities before actually setting up directories, users, and user groups. This section outlines the use of these utilities, describes the EPA-standard server configuration, and explains how these utilities are used to create user accounts and user groups.

Using SYSCON

The SYSCON program is used to create users and groups, and to assign directory rights to them. A complete description of the operation of SYSCON can be found in Chapter 4 of the Supervisor Reference Manual and Chapter 2 of the Menu Utilities Manual. Basically, the use of SYSCON involves selecting options on layers of pop-up menus until the action desired is displayed on one of the menus.

SYSCON is a powerful program that integrates many of the NetWare command line utilities in addition to providing a few unique services of its own. Many of the functions available in SYSCON allow the user to display the current parameters for a

topic. In order to use the SYSCON functions to add, delete, or modify many of the parameters, the user must have trustee rights equivalent to those of the user Supervisor. Figure 8-1, SYSCON Functions by Authorization, contains a list of SYSCON functions and the rights they require.

SYSCON is invoked by typing SYSCON at the DOS prompt while logged in to a server. Its main menu appears as follows:

Accounting
Change Current Server
File Server Information
Group Information
Supervisor Options
User Information

Explore these menu options while referring to the Menu Utilities and Supervisor Reference manuals. Be careful not to delete users or groups, don't initially change the System Login Script or any account profile defaults, and remember that the ESC key will back you out to the next higher-level menu.

An explanation of the menu options follows:

1. Accounting, if installed, provides charge-back capability according to LAN resources utilized. Its use is not recommended under normal circumstances for two reasons. First, most Agency LAN's are intradepartmental systems in which charge-back serves no purpose. Second, deciding what to charge for, how much to charge, and how to handle interdepartmental billing can become a difficult and time-consuming effort, especially in a Government setting.

2. Change Current Server allows SYSCON functions to be performed on other servers on the Internet.

Task	Authorization
List servers logged in	Any user
Log in to additional servers	Any user
Select current server	Any user
Change to different user of current server	Any user
Change current server	Any user
Log out of server	Any user
List known NetWare servers	Any user
View NetWare server information	Any user
List server groups	Any user
Create/rename/delete server group	Supervisor
View a group's full name	Any user
Assign/change a group's full name	Supervisor
View a group's ID	Any user
List a group's members	Any user
Add user to a group	Supervisor
Delete user from a group	Supervisor
Assign group trustee rights in a directory	Supervisor
Modify/delete group's trustee rights	Supervisor
List users	Any user
Create user on a file server	Supervisor
Rename/delete user	Supervisor
View own full name	Any user
Assign/change user's full name	Supervisor
View user's group membership	Any user
View/create/modify personal login script	Any user
View/create/modify any user's login script	Supervisor
View/modify system login script	Supervisor
Change own password	Any user
View/assign/change any user's password	Supervisor
View security equivalences	Any user
Assign security equivalence to a user	Supervisor
Delete user's security equivalence	Supervisor
View own trustee assignments	Any user
View/assign any user's trustee rights	Supervisor
Modify/delete any user's trustee rights	Supervisor
View user's ID	Any user
Modify account restrictions	Supervisor
Install/modify Accounting	Supervisor
Modify login time restrictions	Supervisor
Edit system AUTOEXEC file	Supervisor
Designate console operators	Supervisor
Set intruder detection and lockout	Supervisor
View server error log (NET$LOG.DAT)	Supervisor

Figure 8-1. SYSCON Functions by Authorization

3. File Server Information shows various data about the server, such as which version of NetWare is currently installed, etc.

4. User Information and Group Information are explained under User Accounts, Groups, and Directory Structures, Page 8-9.

5. Supervisor Options, when selected, presents the following menu:

Default Account Balance/Restrictions
Default Time Restrictions
Edit System AUTOEXEC File
File Server Console Operators
Intruder Detection/Lockout
System Login Script
View File Server Error Log

These functions are explained in detail in Chapter 4 of the NetWare Supervisor Reference Manual. If you explore these now, be careful not to change anything unless you're sure changes must be made.

The first two menu selections allow you to set default account and login time restrictions that will apply to all newly-created accounts. Changes made to these defaults will not affect accounts already created, so that if such changes are to be applied to all existing accounts, you must change each parameter user-by-user by selecting "User Information" from the SYSCON main menu and working down the list.

1. Default Account Balance/Restrictions

Effective January 1, 1990, the Agency-standard account restrictions will be:

Account Has Expiration Date:	No
Limit Concurrent Connections:	Yes
Maximum Connections:	1
Require Password:	Yes
Minimum Password Length:	6

Force Periodic Password Changes:	Yes
Days Between Forced Changes:	90
Limit Grace Logins:	Yes
Grace Logins Allowed:	6
Require Unique Passwords:	Yes

Passwords - no less than 6 characters in length.
Password expiration time - no greater than 90 days.
Unique passwords will be required (system prevents the reuse of the last 8 passwords).

2. Default Time Restrictions

By setting login time restrictions, the LAN Administrator can prevent new logins during specified hours or days of the week. Note that if a user is already logged in and his allowable login time passes, NetWare will not automatically terminate his connection; it will send a message requesting that he log out as soon as possible.

3. Edit System AUTOEXEC File

File server console commands entered in this file (AUTOEXEC.SYS in the System directory) will be executed when the file server boots up. This capability is normally used to establish printer mappings that differ from the NetWare default mappings. If there's no AUTOEXEC.SYS, NetWare automatically creates print queues that correspond to the printer ports defined when the operating system was generated (that is, PRINTQ_0 is assigned to Printer 0, PRINTQ_1 to Printer 1, etc.). However, if AUTOEXEC.SYS is present, NetWare does no automatic mapping, so the mappings must be explicitly stated within AUTOEXEC.SYS.

4. File Server Console Operators

This selection allows the LAN Administrator to designate other users as "console operators" so that they can perform most FCONSOLE operations.

5. Intruder Detection/Lockout

NetWare can detect unsuccessful login attempts if so instructed using this screen. Effective January 1, 1990, the Agency-standard intruder lockout parameters will be:

Detect Intruders:	Yes
Incorrect Login Attempts:	4
Bad Login Count Retention Time:	1 day
Lock Account After Detection:	Yes
Length of Account Lockout:	40 days

6. System Login Script

This function accesses a file (NET$LOG.DAT in SYS:-PUBLIC) which contains commands that are automatically executed by all users when logging on to the currently selected file server. Appendix A of the Supervisor Reference Manual contains descriptions of all the commands and variables that can be used in a login Script. EPA-standard file servers are shipped with standard Scripts which do not ordinarily require modification. But, if a Script must be changed, extreme caution should be exercised.

7. View File Server Error Log

This function allows the LAN Administrator to browse or erase the contents of the file server error log. Recorded errors include bridge router errors, "server down" broadcasts and ring numbering conflicts on the Internet, account lockouts initiated by the server, and others. Virtually all are documented in the System Messages Manual.

The Lan Administrator should check this log occasionally, taking corrective action when necessary, and should clear the log after problems have been rectified.

Implementation of these password and intruder lockout restrictions will bring the Agency's LAN's into conformance with the increased security requirements that have been instituted on other EPA systems.

Using FILER

The FILER program is a menu-driven utility that is used to create or modify the directory structure on a NetWare server volume. The LAN Administrator should be familiar with all aspects of using the FILER utility.

Chapter 4 of the Menu Utilities Manual contains an excellent writeup of FILER's capabilities. Chapter 5 of the Supervisor Reference Manual details certain FILER functions that can only be accomplished by the network Supervisor. After reading all the information on FILER, practice using it. Create several practice directories and assign trustee rights to the Guest user. Once you are comfortable with FILER, delete all practice directories you created.

FILER implements many of the NetWare command line utilities in addition to providing a few unique services of its own. Users must have appropriate trustee rights in order to use the FILER functions to add, delete, or modify many of the parameters. Various functions require either Supervisor security equivalency; parental rights to the directory to be modified; or appropriate Open, Read, Write, Modify, Create, or Delete rights. Figure 8-2, FILER Functions by Authorization, contains a list of functions and the rights they require:

1. Read-Only and Read-Write

   Normally, application program files and any associated overlay or configuration files should be flagged as read-only. This is sound practice even if only the network supervisor has all rights in the application directories, since it helps prevent the accidental corruption or deletion of important program files.

2. Shareable/Non-shareable

   Files can be designated as shareable or non-shareable, however, assigning a non-shareable attribute to a data file does not prevent multiple LAN users from opening that file simultaneously. The average PC application program opens a file only long enough to read the required data into the PC's RAM, where actual processing takes place. The file is then closed until the application needs to either write

Task	Authorization
View current directory information	Any user
Change directory date and time	Supervisor
View effective rights in a directory	Any user
View directory Maximum Rights Mask	Any user
Change directory Maximum Rights Mask	Parental
View a directory's owner	Any user
Change a directory's owner	Supervisor
Add/delete trustees of a directory	Parental
List files	Any user
Delete files	Delete
Rename files	Rename
View file attributes	Any user
Add/delete file attributes	Modify
Copy a file	Open/Create/Del
View a file's creation date	Any user
Change a file's creation date	Supervisor
View a file's last accessed date	Any user
Change a file's last accessed date	Supervisor
View a file's last modified date/time	Any user
Change a file's last modified date/time	Supervisor
View a file's owner	Any user
Change a file's owner	Supervisor
View a file's size	Any user
View a file's contents	Read/Open
View/change the current directory path	Any user
Display General Defaults Menu	Any user
Specify file copy/delete confirmation	Any user
Specify file overwrite confirmation	Any user
Specify directory in/exclude patterns	Any user
Specify file in/exclude patterns	Any user
Add/delete file search attributes	Any user
Rename a group of subdirectory names	Parental
Rename/Delete subdirectories & names	Parental
Add subdirectories	Parental
View subdirectory creation date/time	Any user
Specify Maximum Rights for multiple dirs	Parental
Specify owner for multiple subdirectories	Parental
View a subdirectory's maximum rights	Any user
Change a subdirectory's maximum rights	Parental
View a subdirectory's owner	Any user
Change a subdirectory's owner	Supervisor
Add/delete trustees of a subdirectory	Parental
View volume information	Any user

Figure 8-2. FILER Functions by Authorization

changed data to the file, or read other data from it. WordPerfect is an excellent example of the difference between standalone and LAN-compatible applications. In its standalone version, WP does not hold a document file open while it's being edited, so there's no way to prevent multiple LAN users from editing the file simultaneously. Its network version does lock document files opened during editing, thus alleviating this problem.

This is an important point to remember when installing standalone PC applications on the LAN, and it's pertinent only when accessing files in shared directories (specifically, when working in the \USER\SHARE directory).

3. Execute Only

This attribute can be assigned only to .COM and .EXE files, and can be applied only by the network Supervisor. A file so flagged will appear in a directory listing and can be run, but it can neither be copied nor its contents displayed. This attribute can't be subsequently removed; the file must be deleted and recreated by the network Supervisor in order to restore normal file attributes.

4. Hidden

When applied, this attribute prevents the tagged file from appearing in a directory listing. DOS batch files will not run if so flagged, and some application programs are unable to find hidden data files.

5. Indexed

If a file is flagged as "indexed", NetWare will index that file's File Allocation Table (FAT) entry in the server's RAM. The FAT entry for a given file tells NetWare where all the pieces of that file are actually located on the disk drive. For a large file, such a FAT entry might be quite lengthy. Each time the server reads from or writes to a small block of data, the server must scan the entire FAT to find where the data belong. If the FAT entry is large, this scanning process may take some time. Indexing the FAT entry speeds this process considerably.

This suggests that the larger the file (and by extension its FAT entry) and the more often a file is read from and written to, the greater will be the benefit of FAT indexing. Regarding microcomputers, such large, frequently opened files are usually data base files.

Novell recommends that this attribute be applied only to files of 2 Mb or larger. Exercise restraint in using this feature because each indexed file causes the server to reserve a portion of RAM that could be used for other purposes.

USER ACCOUNTS, GROUPS, AND DIRECTORY STRUCTURES

After the network operating system software has been installed and before application programs are loaded, the server's directory structure and user access and security must be specified. Just as planning the network topology is an essential step in installing network cabling and hardware, planning the server file organization and user access is necessary for the successful installation of application software.

The steps involved in preparing the server for application software and user operation include:

1. Planning.
2. Creating a directory structure on the server (FILER, MKDIR).
3. Creating user profiles, including passwords (SYSCON).
4. Specifying user, directory, and file security (SYSCON, FILER).

To complete these steps, you must thoroughly understand DOS directory structures and the NetWare programs FILER and SYSCON. Users are added and given access to certain directories by using the SYSCON program.

DOS directory structures are covered in detail in both the DOS manual and the NetWare User's Guide. In general, a directory can be thought of as having an inverted tree or hierarchical structure. That is, there is a top-level directory (referred to as the "root" directory) from which branch other directories, each of which

may contain additional subdirectories, and so on. The advantage of this type of organizational structure is that it allows the program files for each application to be kept in their own directory. Within EPA, this is achieved by creating a separate directory for each application under \APPS. Data files are usually stored in the users' "home" directories located under \USER. Thus, the directory structure on a standard EPA server generally appears as shown in Figure 8-3.

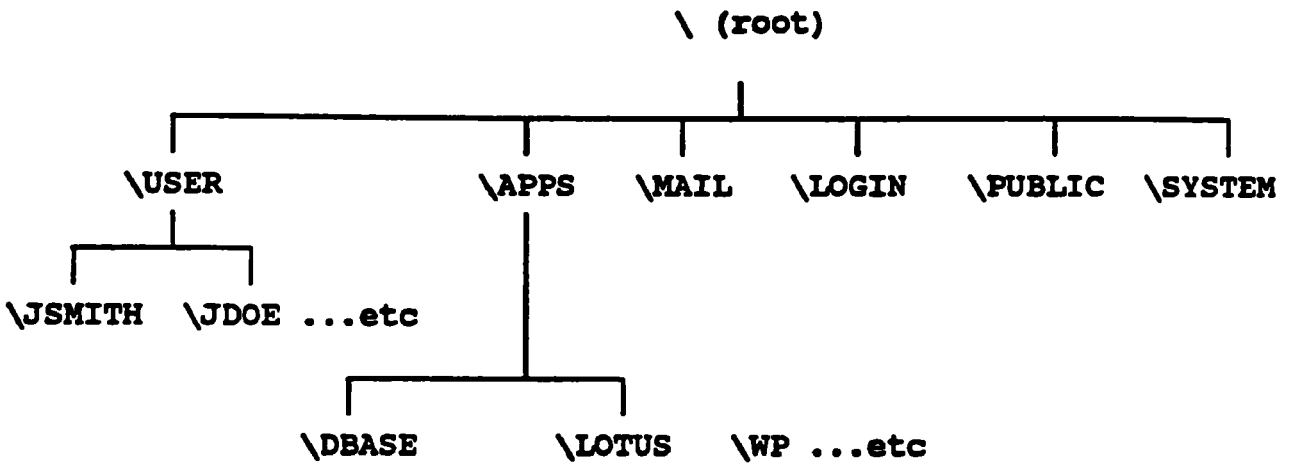


Figure 8-3. Directory Structure on Standard EPA Server

This structure places all dBASE program files in \APPS\DBASE; LOTUS 1-2-3 files in \APPS\LOTUS; WordPerfect files in \APPS\-WP; etc. Data files reside in the user's home directory. For John Smith, for example, that would mean \USER\JSMITH. The MAIL, LOGIN, PUBLIC, and SYSTEM directories are automatically created and loaded by NetWare when the operating system is installed and, generally, their contents should not be modified.

Each user on a network will need to maintain a directory of files to which only that user will normally have access. These personal directories are grouped together under a single directory called \USER and are named according to user login names. For example, John Smith, whose login name is JSMITH, is assigned all rights in \USER\JSMITH. This directory is referred to as the "home" directory, and is the default data file directory for most

LAN applications. The standard system login script assigns drive letter F: to this directory.

Following this strategy, if directories are needed for specific groups of users, the directory \GROUP should be created along with subdirectories whose names correspond to the groups assigned to those subdirectories. For example, if the Water Management Division has its own server and the Wetlands section requires private storage, a group called WETLANDS and a directory called \GROUP\WETLANDS would be created on that server. Everyone in the Wetlands section would be added to that group, which would then be assigned trustee rights in the \GROUP\WETLANDS directory. If you wanted the system to automatically assign a drive letter to that directory when group members logged in, you could insert the following command in the system login script:

```
IF MEMBER OF "WETLANDS" THEN MAP H:=SYS:GROUP/WETLANDS
```

(This command is described in Appendix A of the Supervisor Reference Manual.) From then on, any user added to the Wetlands group would automatically have access to the \GROUP\-WETLANDS directory and would, upon logging in, have that directory mapped as Drive H:.

Shared files are kept in the \USER\SHARE directory, which is mapped as Drive G: by the EPA-standard login Script. All LAN users have unrestricted access to this directory; they can create, delete, and modify files at will, regardless who originally created those files. Therefore, this directory will have to be purged regularly.

TROUBLE-SHOOTING

The FCONSOLE menu utility first appeared with NetWare 2.1. It provides some server console services, such as the ability to down the file server or clear a connection. Its main purpose, however, is to provide statistics regarding file server performance, especially memory and disk usage. Through regular monitoring, the LAN Administrator can determine when a server is not performing efficiently and take corrective action.

The network Supervisor can perform all FCONSOLE functions. He can also designate LAN users as console operators (via SYSCON),

and they can then perform all FCONSOLE functions except to down a server or clear a connection. Thus, the descending chain of FCONSOLE rights is (1) Supervisor, (2) console operator, (3) and LAN user. Ordinarily, LAN users have very little authority in FCONSOLE.

Figure 8-4 contains a list of FCONSOLE functions and those authorized to use them.

Task	Authorization
Broadcast console message	Console operator
Change current file server	Any user
View connection information	Any user
Clear connection	Supervisor
Take down file server	Supervisor
View file/lock activity on server	Console operator
View LAN driver information	Any user
Purge all salvageable files	Console operator
View server statistics	Console operator
Enable/disable new logins	Console Operator
Change data and time on server	Console Operator
View NetWare version information	Any user

Figure 8-4. FCONSOLE Functions by Authorization

FCONSOLE is invoked by typing FCONSOLE at the DOS prompt while logged in to the network. Its main menu appears as follows:

Broadcast Console Message
Change Current File Server
Connection Information
Down File Server
File/Lock Activity
LAN Driver Information
Purge All Salvageable Files
Statistics

Status
Version Information

Explore these functions while referring to Chapter 9 of the Supervisor Reference Manual. Be careful not to (a) down the server, (b) broadcast a console message, which could interrupt work in progress at a user's machine), (c) clear any active server connections, or (d) disable logins, which can be done within the "Status" function). The LAN Administrator will be primarily concerned with information provided by the "Statistics" function.

This area encompasses a wealth of information, all of which is explained in the manual. The following concentrates on locating data which allow the LAN Administrator to determine if and what corrective action needs to be taken to improve file server performance.

Summary Screen

The following four categories of information appear on this screen:

1. Disk Requests Serviced from Cache. This percentage indicates how often file server disk read requests from all workstations have been serviced directly from the server's RAM. It should fall between 95 and 99 percent. If the percentage is lower, system RAM should be expanded. (Run NETGEN afterward.) The baseline Agency file server with 2 Mb of RAM and 70 Mb of disk will average 97 or 98 percent when standard OA applications are run from it. If disk capacity is expanded greatly or if disk-intensive applications such as WasteLAN are added, this percentage may drop precipitously.

2. Routing Buffers - Maximum and Peak Used. The file server can process a certain number of read or write requests simultaneously. Additional requests are stored in "routing buffers." If the server is busy and all routing buffers are full, requests are placed on hold and network performance drops. Thus, if the "Peak Used" approaches or matches the Maximum, the number of available routing buffers should be increased. This can be accomplished by specifying a greater number of communication buffers

when running NETGEN (see NetWare 286 Installation, Page 4-80, and NetWare 286 Maintenance, Page 2-52).

3. Open Files - Maximum and Peak Used. This number represents the total number of files simultaneously held open by all workstations on the LAN. If the maximum number of open files reaches the limit and a workstation tries to open additional files, the attempt will fail and that workstation will be placed on hold until either file handles are released elsewhere, or the shell times out (an error condition). Therefore, if the "Peak Used" number approaches or matches the maximum, the maximum number of open files allowed should be increased. This can be accomplished by specifying a greater number of open files when running NETGEN (see NetWare 286 Installation, Page 7-41, and NetWare 286 Maintenance, Page 7-11).

4. Connections - Maximum and Peak Used. Advanced Netware 286 allows up to 100 active attachments to a file server. (Attachments are defined as workstations that are either logged in to a server or attached to that server while logged in on another.) If the peak number of connections used approaches or matches 100, another file server should be set up to accommodate part of this large pool of users.

5. Cache Statistics Screen. This screen presents detailed information about server cache performance and related disk reads and writes. Of all of these, only the "Trashing Count" may indicate a remediable problem (see Netware 286 Supervisor Reference, Page 9-46). If this count exceeds 0, server RAM must be expanded. The probable cause of disk thrashing is insufficient server RAM for the total amount of disk storage installed, combined with heavy server usage. For example, if a 380 Mb disk were added to a standard Agency file server without adding RAM, thrashing would result when large numbers of files were opened by many LAN users simultaneously.

6. Disk Statistics Screen. A rapidly escalating "I/O Error Count" could indicate a dying server disk channel. This becomes increasingly likely as the file server hardware ages.

7. File System Statistics Screen. A high number of "Fatal FAT Write Errors" may indicate a degenerating disk controller or drive. However, this is a more critical problem because a corrupted file allocation table will cause the affected files to be unlocatable. Up-to-date backups will allow you to recover these lost files.

9. BRIDGES

OVERVIEW

A bridge is generally defined as a connection between two networks that use the same communication method, the same kind of transmission medium, and the same addressing structure. There are two basic types of NetWare bridges: internal and external.

Internal bridges are those most commonly used throughout the Agency. Internal bridges are installed and operate on the file server itself. Functionally, they are identical to external bridges, but are installed in the file server at system generation time when the server is received by the user. Since a system generation is required to install an internal bridge, anyone having this requirement after receiving their file server should contact LANSYS for assistance. Since internal bridges are rarely installed on existing file servers, only external bridges are discussed in this document.

An external bridge is one that runs on a workstation that does not perform as a file server. When an external bridge is used within the cable limitations for a network, it is called a LOCAL bridge. If the bridge is used outside the cable limitations, it is called a REMOTE bridge. External bridges can be operated in the dedicated (bridge only) mode or the non-dedicated (bridge and workstation) mode.

EXTERNAL BRIDGES SHOULD BE OPERATED ONLY IN THE DEDICATED MODE SINCE USING A BRIDGE AS A WORKSTATION WOULD CAUSE BRIDGE FAILURE IF THE WORKSTATION HAD TO BE RE-BOOTED FOR ANY REASON.

Documentation

The reference manual used throughout this document is the Novell External Bridge Supplement (172/Rev1.00) which is supplied with Advanced NetWare V2.15.

INSTALLATION

Local Bridges

Local bridges are normally used to connect workstations on one floor of a building to a server on a different floor. This is usually accomplished via the building backbone. For example, a file server and it's associated workstations are located on the 10th floor of the building. This file server is also internally bridged to the building backbone. You would like to add users on the 11th floor to the file server on the 10th floor. To properly accomplish this, you would have to add an external bridge on the 11th floor. You would actually be setting up an additional user ring on the 11th floor without adding a file server. You would first have to install two token-ring adaptor boards in the bridge: One connected to the backbone and the other to the newly created user ring. You must then generate the software for the bridge. The reference manual discusses software generation in detail starting on Page 2-1. Follow the instructions in the manual for bridge generation keeping the following facts in mind:

1. Always select the IBM token-ring LAN drivers for LAN A and LAN B.

2. The token-ring adapter card connected to the building backbone should be assigned the network address of the backbone.

3. The token-ring adapter is connected to the newly created user ring. The network address for this ring should be obtained from LANSYS. Do not arbitrarily choose a network address.

By following the instructions for bridge generation, you have generated the software for use as a Local bridge. To activate the bridge, copy the BRIDGE.EXE file created during the bridge generation to the boot disk of the bridge PC. Reboot the PC using the BRIDGE.EXE instead of the IPX.COM. When both LAN A and LAN B have been initialized and the colon prompt has been received on the bridge PC screen, the bridge is active.

Remote Bridges

Remote bridges are used to connect a group of workstations that are outside the token-ring cable limitations to a file server. A remote bridge requires some type of connection medium, such as

modems and a phone line. For example, to connect a group of three workstations in one building to a file server in another building across town would require one bridge PC at each location. The bridge at the file server location would have one token-ring card attached to the local server ring and a modem connected to a phone line. The bridge PC at the remote location would be identically configured, with the token-ring card attached to the local ring for the three workstations and a modem attached to a phone line. On each of the bridge PC's, the modem would connect to the COM1 or COM2 ports. For the bridge PC at the file server location, you would follow the instructions for Bridge software generation with the following exceptions: The driver for the local file server ring will be the token-ring LAN drivers. The driver for the modem connection must be IBM ASYNC (COM1/-COM2).

Once the BRIDGE.EXE has been successfully generated, you will have to configure the bridge software for a remote connection. This is covered in Section 3 of the reference manual. This process allows you to configure the LAN driver and the modem you will use for the remote bridge connection. Since modems and a phone line are being used for the bridge, be sure to set up the file server bridge PC to receive calls to activate the bridge from the bridge PC at the remote location.

To set up the bridge at the file server location, run the ARCONFIG program in accordance with instructions beginning on Page 3-1 of the reference manual. These instructions provide all the information you will need to configure the bridge software.

After the server bridge PC software generation has been completed, you will have to generate the workstation shell to be used in the bridge PC at the remote location. This is covered in detail starting on Page 6-1 of the reference manual. When generating the remote bridge PC shell, be sure that the remote bridge initiates all calls.

As you can see, when a remote dial-in type bridge is prepared for use at the file server location, different remote bridges can dial into the file server bridge. This can be particularly useful when only occasional file server access is required from different locations.

When you have connected a group of remote workstations to a file server through a remote bridge, you must remember that your connection to the server is now running at modem speed and not token-ring speed. This will result in considerably slower response at the workstation. To help decrease the time it takes to load programs into the workstation from the server, copy as many program files as possible to the workstation prior to attaching it to the server. For example, if the LOGON program is copied onto the workstation, it does not have to be loaded from the server over the phone line to the workstation, resulting in a considerable time savings. This would be true for any programs that you would run in the workstation.

OPERATION

Once a bridge is operational, daily operational intervention is not required. A bridge will remain up until the PC on which it resides is either taken down or a hardware problem is encountered. In the case of a local file server bridge connected to the building backbone, the bridge PC will remain functional even if the server goes down.

TROUBLE-SHOOTING

Local Bridges

Troubleshooting of local bridges is rarely difficult. First, check the token-ring cable connections to both the Multi-station Access Units (MAU's) and the connections on the back of the bridge PC. Next, check the token-ring cards for proper operation. Run the diagnostics on the token-ring card from the diskette that came with the card. If the bridge still will not operate, check the software GEN for proper BRIDGE.EXE generation. Then, check the PC itself to assure that the PC is functioning properly.

Remote Bridges

Troubleshooting remote bridges is basically the same as with local bridges. The only difference is the addition of the modems and the phone lines. Occasionally, phone lines can be noisy and cause connection problems. If the remote bridge does not make proper connection with the file server bridge PC, bring up the remote bridge a second time. If problems persist, check the modems for proper setup. The setup of the modems will vary from manufacturer to manufacturer.

10. WORKSTATION HARDWARE

OVERVIEW

Workstations are personal computers operated by network users. They are used much like ordinary, non-networked computers - each processing its own files and using its own Disk Operating System (DOS). A NetWare "shell" is loaded into each workstation to enable it to communicate with the file server and other stations on the network.

Any Agency standard IBM PC/XT, PC/AT, PS/2, Telex PC, Epson Equity III, or 100% IBM-compatible PC may be used as a LAN workstation. Hardware requirements for these workstations on a network running Novell Advanced NetWare 286 are 640 KB RAM, the appropriate network interface card, and at least one floppy drive. If you are installing only new equipment ordered from the SMA or FDC contracts, then all of the workstations will meet the minimum requirements. However, if you plan to use existing computer equipment on the network, the equipment must be upgraded to 640KB RAM, DOS 3.1 or later, with a network interface card to operate the NetWare workstation software.

INSTALLATION

All personal computers on the network must have a Network Interface Card (NIC). An AT standard bus PC (such as a Telex 1280, Epson Equity III+, or IBM PS/2 Model 25 or 30) being used as a workstation must have a Token-Ring Adapter II card. Workstations on the network with the new microchannel bus architecture (PS/2 Models 50, 60, 70, or 80) are required to have Token-Ring Adapter/A cards. In addition, an IBM Token-Ring Network PC Adapter Cable, or, if your network uses telephone twisted pair media, a Type 3 Media filter, will be needed. All items are available on the SMA contract.

Each IBM Token-Ring Adapter/A or Adapter II card is shipped with an IBM Token-Ring Network PC Adapter Hardware Reference Library Guide to Operations (TRN GTO) Manual and a diskette containing configuration files and adapter diagnostics. The manual provides information relevant to configuring and installing the NIC and must be referenced during installation.

Adapter/A Card Installation

If you are installing the Adapter/A card in a PS/2 Model 50, 60, 70, or 80, then the first step of the installation process will be to copy configuration files supplied with the card to the IBM Product Two Diskette (Reference Disk). These files will be needed to reconfigure the system for the Adapter/A card. The Installation Instruction Manual supplied with the Adapter/A card provides procedures for copying the proper configuration files, installing and testing the card, and problem solving. These procedures should be followed step by step to ensure proper installation and testing of the Adapter/A card and Adapter cable. If problems are encountered, refer to the Troubleshooting Section of the manual.

Adapter/II Card Installation

For network workstations that have the standard AT type bus, an Adapter/II type card must be installed. These cards contain a series of switches which configure the hardware to work appropriately with the software and other hardware present in the machine. Refer to the Guide to Operations Manual for a detailed description of these switches and their proper settings. Under most conditions, the default settings referred to in the manual are appropriate. Exceptions occur when other expansion cards are installed, and when interrupts and or ROM/RAM addressing conflicts occur. In these cases, non-conflicting Interrupt and ROM/RAM address selections must be made using Appendix B of the Guide to Operations, along with documentation pertaining to the other expansion cards. The Agency LAN Bulletin Board provides information on settings for typical Agency configurations. (i.e., Intel Above Board, Vega Board, etc.)

Chapters 2 and 3 of the Guide to Operations Manual contains detailed installation and testing procedures for the Adapter/II card. These procedures should be followed to ensure proper installation.

OPERATION

It is important that the Token-Ring Diagnostics be run on each workstation. Proper independent verification of each workstation can make networking problem determination easier by eliminating problems caused by faulty workstation hardware connected to the network.

Users should be familiar with the proper use of their workstations in a LAN environment. They should be requested to report any abnormalities to the LAN Administrator for analysis. No other special operating procedures are required.

TROUBLE-SHOOTING

Interrupt conflict errors usually show up as workstation "hangs." In most cases, Interrupt IRQ2 (default setting) is appropriate. An exception occurs with the Epson Equity III, which should be changed to IRQ3 for best results.

LAN Administrators can isolate most workstation hardware problems by using the following general guidelines:

1. In many cases, a thorough visual inspection of the equipment can save much time and effort by revealing problems that have been self-induced. These problems usually arise after moving equipment, installing cards, etc. Go over the equipment, thoroughly checking for loose or improper cable connections, or other items that may have been knocked loose. If the cover to the equipment was removed, check the inside as well.

2. If the equipment was operating normally prior to installation of cards or changes to parameters or switches, consider these changes as causing the problem. It may be necessary at times to restore the equipment to its original configuration and repeat the installation procedure.

3. If errors occur only while attached to, or attempting to attach to the network, then it is reasonable to assume that the problem is associated with the adapter card, its cabling to the network, or possibly the switch or parameter settings selected. The adapter card and all cabling through to the MSAU should be tested. This can be done by removing the workstations data connector at the MSAU and running the Adapter Diagnostics as outlined in Chapter 3 of the Guide to Operations.

4. The System Diagnostic Routines received with the equipment can be used to isolate a hardware problem. Operating procedures for these routines are contained in manuals received with the system. When running these routines, it

may be necessary to remove expansion cards that may be foreign to these diagnostics.

Adapter Diagnostics

1. Turn the power switch on the workstation to OFF.

2. If your network uses the IBM Cabling System data grade media, leave the cable attached to the NIC in the computer, but disconnect it from the network (typically at the MAU or wall plate connections). The connectors are self-shorting when not installed.

   If your network uses telephone twisted-pair media, disconnect the Type 3 Media Filter from the NIC. Install the wrap plug (attached to the Type 3 Media Filter) onto the NIC.

3. Insert the Training Diagnostics diskette into floppy Drive A: and close the drive door.

4. Turn the power to the workstation ON.

5. The TRN Diagnostics should load and the Copyright/Diagnostics Option screen should appear. Follow instructions on the screen to run the diagnostic routines.

6. Select Option 0, Run Diagnostic Routines. The screen should indicate which Token-Ring Adapter(s) are installed in the computer. Verify whether the list is correct.

7. You can select whether or not to run the tests once or several times, or to log errors to a disk file or a printer (if connected). Select an appropriate option to run the diagnostic routines.

8. The screen will display the following status information:

   Adapter Address
   Code Level
   Interrupt Level
   ROM Address

Verify that the information above is appropriate for the station's NIC. The screen will prompt for the appropriate cable configuration for your network adapter (PC Adapter Cable or Modular Telephone Plug). Select the appropriate response and verify that the adapter cable is not connected to the network.

Beneath the status information, the diagnostics will display any information pertaining to testing status and error messages received during the tests. If an error is detected, the error message is displayed after the testing status message.

If an error occurs, refer to Chapter 3 of the Token-Ring Network Guide To Operations Manual for a detailed explanation of the error message and appropriate actions to take for each type of error.

11. WORKSTATION SOFTWARE

OVERVIEW

Workstations and the network file server communicate by means of software called the "NetWare shell". The shell must be loaded into each workstation before the workstation can function on the network. The NetWare shell has two parts: NET3 or NET4 and IPX.

NET3 or NET4 (depending on the DOS version you are using) is responsible for directing workstation requests to DOS or NetWare. When a command is entered at a workstation, the shell decides if it is a workstation task (to be directed to DOS) or a network task (to be directed to NetWare). If the request is a network task, then the second part of the shell, Internetwork Packet Exchange (IPX), will be called to send the request to the file server or, in some cases, directly to other network stations.

The remaining software required in this network communication process is referred to as the Adapter Support Interface (TOKREUI or DXMxxMOD device drivers). This is the code used to interface IPX with the token-ring adapter card to send the request in packet form across the network.

All files necessary for installing and configuring the networking software on an individual workstation have been included on the SMA Workstation Installation disk received with each network file server.

INSTALLATION

Using the Installation diskette received with your network file server, follow the procedures given to install the networking software.

The following discussion presumes that the network interface card and the network cabling have been completed for this workstation.

1. If the workstation is a PS/2, PC/XT, or AT-compatible with a hard disk, insert the workstation setup disk into workstation diskette Drive A.

If the workstation has no hard disk, then insert the Installation diskette in Drive A:, and proceed to Step 3.

2. Type A:INSTALLW and press ENTER. The INSTALLW batch file will perform the following steps:

```
COPY A:\AUTOMAXX\*.* C:\
COPY A:\WORKSTAT\*.* C:\
MD NETWORK
COPY A:\NETWORK\*.* C:\NETWORK
```

This procedure will install the AUTOMAXX menu on the workstation hard drive, configuring the system as a network workstation.

3. The files to be attached to the network are located in the \NETWORK directory (at this point on Drive C: or Drive A: if there is no hard drive.)

For machines running DOS 3.3 or greater, the required files are:

```
IPX.COM
NET3.COM    (NET4.COM FOR DOS 4.X)
ANSI.SYS
DXMA0MOD.SYS
DXMC0MOD.SYS
```

For AT-compatibles running DOS 3.1 or 3.2, the required files are:

```
IPX.COM
NET3.COM
ANSI.SYS
TOKREUI.COM
```

At this time, the appropriate files should be copied to the root directory of the boot disk, using the DOS copy command.

4. Create or modify the existing CONFIG.SYS file for the workstation to adapt it to the network operating environment. The CONFIG.SYS file should contain the following

statements: (If a CONFIG.SYS file already exists, ensure that any necessary lines in the old file are retained in the new copy of CONFIG.SYS).

```
BUFFERS = 40
FILES = 25
DEVICE = ANSI.SYS
```

If running DOS 3.3 or greater, also include:

```
DEVICE = DXMA0MOD.SYS
DEVICE = DXMC0MOD.SYS
```

See Page 11-4, Customizing CONFIG.SYS FILE, for more information.

5. A batch file should be created at this time to execute the commands in the proper sequence for connection to the network. To automatically go to the network when the batch file is executed, use a standard text editor to create a batch file containing the following statements:

```
PROMPT $p$g
CLS
TOKREUI  (Include only for DOS 3.1 or 3.3)
IPX
NET3
F:
LOGIN
```

6. At this point, the machine should be rebooted and checked for proper connection to the network. A normal display showing proper connection will be as follows:

```
Novell IPX/SPX V2.1x
(C) Copyright 1985, 1986 Novell Inc. All Rights Reserved.

LAN Option: IBM Token Ring V2.3
Hardware Configuration: Self Configurable
NetWare V2.1x - Workstation Shell for PC DOS V3.x
(C) Copyright 1983, 1988 Novell, Inc. All rights Reserved.

Attached to server XXX-XXXX
Wednesday, October XX, 19XX    10:02:36 am
```

OPERATION

The EPA AUTOMAXX Menu system contained on the SMA Installation disk should be installed if a hard disk is available at the workstation. The menu system will prompt users through the login procedures in a user friendly manner. Follow the instructions as outlined on the SMA Installation disk.

Customizing CONFIG.SYS

The CONFIG.SYS file is a standard text file, and any text editor can be used to create or edit this file.

When a PC is powered on (or rebooted using CTRL-ALT-DEL), DOS reads a special file in the root directory which tells it how to configure the system for the desired operations. The number of open files and the number of buffers available to DOS are among many parameters which can be modified by editing the file.

Many programs that run under the DOS environment often require that several files be open simultaneously. Additionally, the network shell running on a workstation requires added file access. The default DOS number of open files is 8. A value between 20 and 40 will result in better performance for network use.

DOS will allocate a specific number of buffers to be used in storing the most recently transferred data between memory and the disk. The more buffers DOS has, the more data can be stored and the fewer disk I/O requests are necessary. The default DOS number of buffers is 2. A value between 16 and 30 is appropriate for most network use, depending on the applications which will be run from the workstation. If a user complains of poor network disk access performance, you should increase these values.

It may be necessary, in instances where large programs do not have sufficient memory, to reduce the "FILES" and "BUFFFER" statements in order to make more memory space available. The "DEVICE=ANSI.SYS" statement could also be eliminated in some cases. (IPX.COM uses approximately 19K, and NET3 uses approximately 38K bytes of RAM.)

The CONFIG.SYS file must reside in the root directory of the drive from which the system is booted (A: if a floppy system; or C: if a hard disk system). The parameters and use of the CONFIG.SYS

file are explained in detail in the DOS manual. Refer to the index for CONFIG.SYS. The workstation must be rebooted (with CTRL-ALT-DEL) for DOS to recognize the changes made in the CONFIG.SYS file.

TROUBLE-SHOOTING

Workstation software problems generally result from addressing and interrupt conflicts between the NetWare shell and other Terminate and Stay Resident (TSR) software. After installing new software containing TSR programs, the workstation should be monitored for any abnormal operation.

Special parameters are available for assigning different ROM and RAM addresses to the token-ring adapter card. These addresses may have to be reassigned when other expansion boards are installed in the workstation. See your Token-Ring Network Guide to Operations Manual for instructions to change these parameters.

The Agency LAN Bulletin Board can be referenced for problem descriptions and fixes.

Note: Epson Equity III machines running DOS 3.1 or 3.2 will not run properly on the LAN at 12 MHz speed. Upgrading to DOS 3.3 and installing the DXMxxMOD device drivers corrects this problem.

12. LANSPOOL

OVERVIEW

LANSpool is a printing program used on Novell Networks that allows a network workstation to function as a network print server. Printers are thus able to be placed in more convenient locations without the restriction of being attached to a file server.

LANSpool can be installed in either a dedicated or background (non-dedicated) mode. In dedicated mode, the workstation performs no other function than serving the shared printers. Background mode allows the print server workstation to be used to run other applications while its printer(s) is being shared.

LANSpool works in conjunction with the NetWare file server based print spooler, and operates with NetWare print queues. LANSpool requires minimal RAM overhead from the workstation. Its presence is completely transparent to network users.

INSTALLATION

The following procedures are necessary to install LANSpool on either the dedicated or non-dedicated versions. Network Supervisor or Supervisor-equivalent privileges are needed to complete the installation. Refer to Chapter 2 of the LANSpool Users Manual for more detailed information.

1. Log in to the network as Supervisor and map a logical drive to the volume where you want to install LANSpool.

   ```
   F:\>map g:=fileserver\sys: <Enter>
   F:\>g: <Enter>
   ```

2. Create a directory for LANSpool and copy all of the LANSpool files to it.

   ```
   G:\>md lanspool <Enter>
   G:\>cd lanspool <Enter>
   G:\LANSPOOL> copy a:*.* <Enter>
   ```

   Note: A directory named LANSPOOL was created only as an example. The LANSpool files can be copied to a directory of your choice.

3. Start the NetWare printer utility program PCONSOLE.

   G:\LANSPOOL>pconsole <Enter>

4. Select the PRINT SERVER INFORMATION option from the PCONSOLE main menu. Using the <ins> key, create a name for the new print server.

5. Press <Enter> again to select the new print server. Enter additional information for password and name.

6. Press <Esc> to return to the PCONSOLE main menu and select the PRINT QUEUE INFORMATION option. Using the <ins> key, create a print queue for use with the new print server.

7. Press <Enter> again to select the new print queue. Enter additional information for queue operators, queue servers, and queue users. Refer to the LANSpool Users Manual for specific details on setting these parameters.

8. Use the <Esc> key to exit PCONSOLE and return to the system prompt.

9. Run the LANSpool program GIVEPRIV. Follow the prompts as they appear on the screen.

   G:\LANSPOOL>givepriv <Enter>

   (Note: You will need to run GIVEPRIV every time you create a new print server account or add a new print queue to the network.)

10. Run the LANSpool program SETSERIA. For example:

    G:\LANSPOOL>setseria <Enter>

    The LANSpool program requires that you enter a special code in order for the program to be fully functional. During this part of the installation, you will have to telephone LAN Systems Inc., for a special code in order to properly serialize LANSpool.

11. Proceed to the appropriate section on dedicated or background installation, depending on which implementation you plan to use.

Background LANSpool Installation

The background version of LANSpool allows you to operate a network workstation concurrently as a LANSpool print server and a user workstation. The background version has been implemented as a NetWare Value Added Process (VAP).

The SETNAME program has to be run before actually installing the LANSpool VAP on your server. This program tells the LANSpool VAP which file server, print server, and password you are using. These parameters are the ones that were selected when PCONSOLE was run during the first portion of the installation.

(Note: The file server must be powered down in order for the VAP to be recognized by the system.)

1. Run the SETNAME program. For example:

   G:\LANSPOOL>setname <Enter>

   The program will prompt for the print server name and password that was specified during the PCONSOLE session. If you are installing the VAP on a file server, the SERVER entry should be set to DEFAULT. Save these entries and proceed.

2. Copy the file LANSPOOL.VAP to the SYS:SYSTEM directory. For example:

   G:\LANSPOOL>ncopy lanspool.vap sys:system

   Following the power down/power up sequence, the server will recognize the addition of file LANSPOOL.VAP to the SYS:SYSTEM directory.

3. Log out and take down the file server to which LANSpool and the file LANSPOOL.VAP were copied.

4. Power down the server, then power it up again.

   After the usual screen messages appear, you will see the following message.

   > "Value Added Processes have been defined.
   > Do you wish to load them?"

5. Type "Y."

   You will see a series of messages indicating that the VAP is installing itself.

6. From the workstation at which you plan to run LANSpool, log in to the server that has the VAP installed on it.

7. Go to the subdirectory where LANSpool was installed, and execute the program NODE. For example:

   G:\LANSPOOL>node <Enter>

8. The NODE program will prompt you for parameters particular to the printers attached to the workstation. Refer to the installation section of the LANSpool Users Manual for specific details on selecting these parameters.

   This process - running the NODE program, port selection, queue selection, communications parameter settings, and printer name - must be repeated for each printer to be used in conjunction with the LANSpool server.

9. Press the <Esc> key to exit the setup program. LANSpool will display a message that the Print Server is initialized.

10. Save the settings you selected during installation in an initialization file.

    LANSpool will, by default save your initialization file under the name LANSPOOL.INI on the current working drive and subdirectory. You may, however, change the name and specify a full path name.

This concludes background LANSpool installation. The servers and its queues can now be maintained through NetWare like any other print server on the network. Before incorporating LANSpool into normal network procedures:

1. Ensure that the LANSpool server is responding properly. Test sample output by using the NPRINT or CAPTURE commands.

2. Make a backup copy of the file NODE.EXE in the event that you need to restore the system. This file has been serialized to the NetWare file server.

Dedicated Print Server Installation

From the system prompt for the network drive and directory where the LANSpool programs reside, execute the LANSpool program. For Example:

G:\LANSPOOL>lanspool <Enter>

Utilizing screen prompts, the LANSpool program will ask you for parameters that you created when running PCONSOLE (i.e., file server name, the login name of the print server, and password selected if any).

LANSpool will prompt you for additional information to identify the specific printers to be configured on the print server. Options on each screen can be altered using the <Arrow> keys to make selections and then pressing <Enter>. The default values are correct for a Hewlett Packard Laser Jet printer.

This process - port selection, queue selection, communication parameter settings and printer name - must be repeated for each printer that you plan to use with the dedicated print server.

1. Press the <Esc> key to exit the setup program. LANSpool will display a message that the Print Server is initialized.

2. Press the <Esc> key again. You should now save the settings you selected during installation in an initialization file.

3. Enter a legal DOS filename as the name of the initialization file.

LANSpool will save your settings to the file XXXXX.INI on your A: drive. Later, you may copy this file to the network drive where LANSpool has been installed and use it to configure LANSpool at start up. See the Advanced Features section of the LANSpool Users Manual for more information about initializing files.

This concludes dedicated LANSpool installation. The server and its queues can now be maintained through NetWare just like any other print server on the network.

OPERATION

LANSpool uses normal Netware queuing and print maintenance programs. Consequently, before successfully printing a file, you must redirect output using the NetWare CAPTURE or NPRINT commands.

Using LANSpool in Background Mode

Once the background version of LANSpool has been loaded, its operation will be transparent to the users at the workstation. You can, however, display a monitor for the background version by using the STATUS program. For example:

G:\LANSPOOL>status <Enter>

A menu will appear, allowing you to select detailed information about the printer's configuration and current activity.

Loading Background LANSpool at Boot Time

It is best to automatically load background LANSpool every time a workstation is booted. If this is done, the shared printer(s) will be available for network users at all times when the workstation is on. For example, if a workstation is turned off for some reason, all an end user has to do is restart the machine.

The following procedure will create a special user account that workstations will automatically attach to during booting to load LANSpool.

1. Run the Netware utility program SYSCON. For example:

   G:\LANSPOOL>syscon <Enter>

2. Select the User information option from the SYSCON main menu.

3. Create a new user account. For example, press <Ins> and <Enter>

   PRINT_SERVER <Enter>

   (Note: You can create a user account name of your choice.

4. Press <Enter> again to select the new user, and enter additional information for trustee rights.

5. Select the Trustee Rights option from the User Information menu.

6. Grant Read, Open, and Search rights to the user for the subdirectory where LANSpool has been installed.

7. Use the <Esc> key to return to the system prompt.

8. Copy the following two programs from the SYS:PUBLIC directory to the boot diskette: ATTACH.EXE and MAP.-EXE. Example:

   G:\>copy sys:public\attach.exe A: <Enter>
   G:\>copy sys:public\map.exe A: <Enter>

9. Add the following lines to the AUTOEXEC.BAT file before the line that runs the LOGIN program:

   ```
   attach fileserver\print_server
   map g:=fileserver\sys:lanspool
   map s1:=fileserver\sys:public
   g:
   node lanspool.ini
   a:
   logout
   ```

Note: The subdirectory name, initialization file, file server name, and user account are given as examples only. You can use values of your own choosing. Also, you must have the SYS:PUBLIC directory specified as a search drive before running the NODE program. If the user at this workstation normally boots right into the network, the AUTOEXEC.BAT file can continue with normal login procedures.

Since LANSpool is running as a VAP in the background mode and communicating with the NODE.EXE program at the packet level (not through a user account), you can log out of the network and still have your printer available for other users. This ensures your network security because users don't have to remain logged into the network under their account to share the printer(s) with other network users. As long as the NetWare shell (IPX.COM) remains loaded, the attached printer will be available for other users.

Exiting LANSpool Background Mode

It is not possible to remove the NODE.EXE program from memory without rebooting your PC, but the program can be disabled and your printer returned to a local printer status at your workstation. To remove NODE.EXE and return a printer to a local status, follow these steps:

1. Run the status program. For example, at the DOS prompt type:

   G:\LANSPOOL>status <Enter>

2. Use the <arrow> keys to highlight the printer you wish to remove (if more than one printer has been loaded).

3. Press the <Del> key and select the "yes" prompt to delete the printer.

The printer you selected will be removed from the network as a network printer and returned to a local printer status. The NODE.EXE program is not removed from memory.

Server Console Commands

The background version of LANSpool contains a group of stand-alone commands which report on the status of the VAP. They must be typed from the NetWare server console. The commands and their functions are:

1. LS_DIAGNOSTICS: Displays internal diagnostic information for LAN Systems. (This information may be needed if support is requested from LAN Systems).

2. LS_VERSION: Displays the version number of the LANSpool VAP software that is currently running.

3. LS_STATUS: Displays information about the current state of the VAP. For example:

```
LANSpool VAP Current Status
        File Server:   F/S NAME
        Print Server:  LANSPOOL_VAP
        Printer Nodes in Use: 2
        Queue Nodes available: 27
        Printer 1 is Being Used
        Printer 2 is Being Used
        Printer 3 is available
         etc....
        Printer 10 is available
        Attached to Queues:
                21757973
                66197023
                21365501
```

The number shown after the list of queues is the Print Queue ID#. It can be found in the Print Queue Information menu in the Novell PCONSOLE program. (There are 10 printers and up to 30 queue "slots" available for use with each VAP.)

A list of all LANSpool commands can be obtained by typing VAP at the server console.

Removing the LANSpool VAP

If you want to remove LANSpool as a VAP, delete the file LANSPOOL.VAP from the SYS:SYSTEM directory on the file server where it was installed. Repeat the same procedures at the server level that were required to install the program.

Invoking LANSpool in Dedicated Mode

During normal program invocation, LANSpool will use its own default settings or those found in the file you created during initialization. To invoke the program with a different initialization file, use the name of the file as an argument to the LANSPOOL command. For example,

```
G:\LANSPOOL>lanspool file.ini <Enter>
```

will run the LANSpool program with all of the configuration settings found in FILE.INI. See the Appendix section of the LANSpool Users Manual for details in creating and editing initialization files.

Loading LANSpool during BOOTUP

It is best to set LANSpool to load automatically every time the LANSpool workstation is rebooted. If this is done, shared printers will be available for network users at all times. If the workstation is turned off for some reason, an end user only has to restart the machine.

The simplest way to accomplish this is to have the workstation log in to the network under an account with minimal rights, map to the drive where LANSpool is stored, and run LANSpool. Running LANSpool itself will log the workstation out of the network under that account and log in the station under the print server account. This method is as follows:

1. End the autoexec.bat file for the workstation running LANSpool with the following line:

   ```
   LOGIN SERVER_NAME\ACCOUNT_NAME
   ```

   where SERVER_NAME is the name of the file server, and ACCOUNT_NAME is a user ID.

   The account that you log in under will need to have Read, Open, and Search rights to the directory where LANSpool has been installed. Also, this account should not have a password so that the login procedure will continue automatically.

2. In the individual login Script for this account, map a drive to where LANSpool is installed. For example:

   MAP G:=SYS:LANSPOOL

3. Go to this drive. For example:

   DRIVE G:

4. The last line of the login script should read:

   EXIT "FILE.BAT"

   where FILE.BAT is a DOS file containing:

   LANSPOOL LANSPOOL.INI

   where LANSPOOL.INI is the initialization file you wish to run for a particular workstation.

   Note: Novell limits the exit command to 14 characters in a login Script. You need to exit to a batch file and cannot exit directly to LANSpool with an initialization file specified.)

Upon booting the workstation, the AUTOEXEC.BAT file will log in the workstation under a specified account. The login Script for this account will run LANSpool. Once LANSpool is run, you will automatically be logged out of the network and relogged in as the print server account.

After all of the printers have been configured, the LANSpool main menu will appear on the screen of the dedicated print server. Selections can be made from the menu to monitor the current status of each printer. Other options available from the menu are to run Novell's PCONSOLE utility and to shut down the print server. See the LANSpool Users Manual for more detailed status information.

TROUBLE-SHOOTING

LANSpool uses NetWare queuing and print maintenance utility programs, such as PCONSOLE, PRINTCON, and PRINTDEF. These utilities are available for troubleshooting LANSpool problems.

LANSpool also provides print server monitoring routines. Refer to the LANSpool Users Manual for details on status displays.

All errors generated by the LANSpool VAP (background mode) will be automatically logged to the file SYS$ERR.DAT that is stored in the directory SYS:PUBLIC. This file can be monitored for error conditions.

The LANSpool NODE.EXE program running on the background mode print server is an interrupt driven TSR program which uses specific hardware interrupts for your parallel or serial card. No other cards or devices can use the same interrupt being used by the shared printer. Interrupt conflicts are most likely to occur when configuring printers to serial ports, as these will use interrupts IRQ3 and IRQ4 which could conflict with some network interface card interrupts.

If using a postscript printer, you will need to decide whether to configure it using hardware or software handshaking (DSR or XON/XOFF). To select hardware handshaking (DSR), you must copy the file PSHARD.TXT from the LANSpool diskette to your printer. For software handshaking (XON/XOFF), the file used is PSSOFT.TXT. See the Appendix of the LANSpool Users Manual for additional information. If problems are encountered after setting up for hardware handshaking, try switching to software handshaking.

When running in background mode, the printer attached to the workstation can no longer be accessed as a local printer by the workstation. You must log in to the network and access it as a network printer.

13. SECURITY

OVERVIEW

As the number of LAN installations continues to grow, so do the amounts of data and programs stored on these LAN's. For that reason, microcomputers pose numerous security issues. When work group PC's are tied together to permit resource sharing, securing these resources requires greater effort than if those PC's were in a standalone environment.

Any one work group LAN may be fairly self-contained. While expansion of the LAN is possible (and probable), the domain in which breaches of security may occur generally remains manageable for the work group System Administrator. User's and applications are known to this Administrator. Undesirable outside influences tend to be less of a factor since the system is somewhat contained.

Once these isolated LAN's are tied together via a facility-wide backbone, physical access among work groups is effected immediately. Access from one previously separated LAN to another is physically guaranteed. No longer is a LAN, as a whole, centrally administered. Processing power and data storage are distributed, but so are access points for those who should not be allowed access. Security concerns are no longer just the concern of one manager in a centralized operation. Security becomes a larger issue for all users and System Administrators. Issues of security in one work group may not be as stringent as those in another work group. However, since access to the resources of one work group can be attained by a user in another work group, some levels of security must be maintained throughout the network. Greater levels of security may be implemented locally as required. Thus, we must consider the high and low end security needs of the Agency's networked community. These requirements must be combined with available methods for safeguarding data in order to find the levels necessary to maintain a secure environment.

How Much Security?

Before considering what must be done to secure the resources of a processing environment, you must consider how valuable the resources are and to whom. Questions to be asked are:

1. If all or part of the data stored on the LAN is corrupted or destroyed, what are the ramifications?
2. How much effort would be required to return the system to its normal level of operation?
3. Should the data be secured only from modification or should it be hidden from everyone but those authorized to see it.
4. Who is allowed access to the data?
5. Who might want access to the data?
6. Are those who would access the data necessarily those who should have access?
7. Is Confidential Business Information (CBI) data stored on the LAN?

The levels of security needed to protect the resources of the LAN are dependent on the answers to these questions. The following explains the points of access in a LAN environment and measures that can be taken to curtail or eliminate access by an intruder. These measures can be used in tandem with your requirements in order to formulate a security plan.

OPERATION

Access Points/ Possible Intrusion

The LAN workstation, most commonly a personal computer, is the unit where most of the work on a LAN is done. It is the most common point for access to the data since nearly all the processing is done at the PC, and software which provides access to the resources of a LAN is loaded from the PC. Once this network shell is loaded, the PC is logically part of the network. A PC user, has access to data stored at the workstation itself and, possibly, to data stored on network file servers. The floppy disk drive of a PC could allow an intruder to remove data from the LAN or allow the intruder to introduce faulty or corrupt data and

applications. Indeed, the floppy disk is one of the most common entry point for the introduction of a virus. Once a PC is "infected," floppy diskettes used on that machine and then on another PC can carry the virus with it. By virtue of LAN interconnection, viruses have yet another avenue in which to spread.

File Servers. The majority of data to be shared by LAN users resides on the network file server. Since this server is essentially a personal computer (IBM PS/2 Model 80), it is subject to the same access problems as any PC on the LAN. The server is generally executing a Network Operating System in dedicated mode. Therefore, to access and corrupt data, the intruder has to physically remove the file server or take the server down in order to first load DOS from the floppy drive. Even though files on a dedicated NetWare server cannot be accessed at the server from DOS, an intruder could format the hard disk. If the server and keyboard are accessible to those other than the Administrator, the server could be powered down or reset.

Cabling MAU's and Wire Closets. Token-Ring networks are actually "star-wired". That is, all nodes are cabled to a central point - the wire closet. One of the things that makes the token-ring attractive is that it allows for nodes to be added without disturbing the network. Unfortunately, this topology permits an intruder to attach to the network undetected. This access could occur at the wire closet or at the wall outlet of an unused run of cable. It is possible for an intruder to place a protocol analyzer on the network at one of these two access points and to trap passwords or data as they are passed along the network. A sophisticated hacker may even "tap" into a particular cable run.

Remote Dial-In and Gateways. Access to a LAN with no connections to the outside world is generally limited to those with access to the facility itself. Once dial-in access to the LAN is provided, the LAN is potentially opened to anyone. If phone numbers for LAN access become known to outside interests, physical access to the LAN is available.

Gateways provide access to resources outside the LAN. If gateways are established without appropriate security measures, then access to the LAN via outside resources can be established.

While there are many similarities between mainframe and LAN security needs, mainframe security is not discussed here.

Securing the LAN

Intruders must gain access to a LAN before they can compromise the integrity of data and programs on the LAN. This section highlights ways in which a LAN can be made more secure and discusses policies already in place which mandate the use of certain security measures. Several methods for securing access points will be given. Some may not need to be implemented, while others are required by policy.

While reading this section, keep in mind the following:

1. Some of the measures recommended may seem to be "over-kill". Before making this determination, be reminded of the questions asked in the previous section. How important is the integrity of the data? How much will it cost to reestablish this integrity in the event of a catastrophic loss? What are the ramifications of data falling into the wrong hands?

2. While EPA has implemented the most effective security programs available, hackers may possibly circumvent these programs. Do not assume that the system is secure.

WORKSTATION SECURITY

The workstation is the point at which a LAN is most frequently accessed. Some methods for securing the workstation are:

1. Use the key and lock provided with the workstation. If the PC must be kept on while the operator is out of the work area, the operator should lock the keyboard.

2. Some PC's provide a ROM-based password routine that is invoked every time the machine is booted. Use the facility if it is available.

3. Several devices which physically prevent the PC from being removed from the work area are available. These include pressure plates and steel cables which anchor the PC to the work surface and locking metal cabinets which physically

surround the PC, allowing it to be locked when the PC is not in use.

4. Depending on the criticality of the data, the room containing the PC can be physically secured. Numerous security systems are available which prevent access to the facility itself (e.g., keycard systems). If Confidential Business Information is processed within the facility, then one of these systems is probably required.

5. Control the use of floppy diskettes. If user PC's are part of a network, then the majority of files which need to be shared should be created and located on the server's disk. Use floppy diskettes only to boot the PC onto the network. If diskettes must be used to introduce data or programs from an outside source:

   - Test the programs on a non-networked floppy drive system. Viruses frequently attach themselves to executable programs on a PC's hard disk. The program should bomb if it attempts to access a non-existent hard disk.

   - Once it is determined that the foreign floppy is safe for introduction to the LAN environment, store it in a central location. Don't allow users to retain these floppies.

   - Back up hard disk data on a regular basis. Should a PC's data be corrupted or lost, it is essential to have a "clean" copy of the data available for restoration.

FILE SERVERS

The Agency standard LAN file server is an IBM PS/2 Model 80. It is a PC. Therefore, the same physical security concerns that apply to workstation PC's apply to file servers as well. Sensitivity is heightened, however, since the server may hold data and programs needed by numerous individuals.

PHYSICAL SERVER ACCESS

The server should be located either in a locked room or should be highly visible to the Administrator or others who are aware of those allowed access to the server.

Once a dedicated server is up and running, the keyboard should be removed or the NetWare Keyboard Lock VAP should be installed. The Lock VAP allows the Administrator to implement password protection at the file server console. For information on installing and using the Lock VAP, refer to the NetWare Console Reference Manual.

LOGICAL ACCESS

After the network shell has been loaded on a network PC, all the resources on the network are potentially available. It is the responsibility of LAN Administrators to ensure that the resources of their LAN's are secure. At the file server, Novell has implemented numerous features within the NetWare 286 operating system which can aid the Administrator in accomplishing this goal. These features are summarized below. Detailed explanations of the use of these features can be found in the NetWare Supervisor's Reference.

Login restrictions are listed below:

1. Required Password. This is required by NDPD LAN Operational Policy 310.09, LAN Security.

2. Minimum Password Length. This option must be set for all users or for individual users. Passwords should be no less than 6 characters in length, containing at least 1 alpha and 1 numeric character.

3. Forced Periodic Password Change. Passwords must be changed at least every 90 days. This can be facilitated with the aforementioned NetWare feature. The user will be reminded by the Network Operating System (NOS) to change his password and can be forced to change it in order to log in. "Grace" logins can be configured to permit a certain

number of login's after the password has expired. This number should be kept to a minimum.

4. Required Unique Passwords. The NOS will track the last 8 passwords used for any given account and will not allow these to be reused. This feature must be implemented on all LAN's.

5. Intruder Detection and Lockout. The NOS can be configured to detect a number of unsuccessful login attempts. This number can be set by the Administrator. Once the number of failed logins exceeds the number set, the account is disabled either for a defined amount of time or until the Supervisor unlocks the account.

6. Limited Number of Concurrent Logins. By default, NetWare allows the same user ID to be logged into the server more than once concurrently. This option must be set to allow only one concurrent log in session per ID.

7. Station Restrictions. Login attempts for any ID can be restricted by either LAN address or node address. This feature is extremely important in a multiple server/multiple ring environment. Administrators should limit access to their file servers to those users on their ring by default. This restriction can be lifted when specific access is needed by a user on another ring. This feature will help the Administrator adhere to NDPD policies, which state: "On LAN's with multiple file servers, users must have a genuine requirement to access a specific server to be given access. Providing all users with blanket access to all servers for ease of configuration is not allowed."

DIRECTORY/FILE ACCESS

When a user logs in with a valid ID, Novell's directory and file security scheme regulates access to the file system in the following ways:

Directory Rights
Trustee Assignment (By user ID or Group of user ID's)
File Flags

Security Equivalences
Supervisor Rights

Directory Rights. The following access rights can be assigned on a directory-by-directory basis:

R	Read from open files
W	Write to open files
O	Open existing files
C	Create and simultaneously Open new files
D	Delete existing files
P	Parental, which includes: Create, rename, erase subdirectories of the directory Set trustee and directory rights in the directory Set trustee and directory rights in its subdirectories
S	Search the directory
M	Modify file attributes

Trustee Assignment. The above rights can be assigned for a particular directory by user ID or Group ID. This method of granting access is called assigning Trustee Rights. For example, a user named USER1 could be given Read, Write, Open, Search, and Create trustee rights for the directory SYS:APPS\DBASE. Furthermore, if several users needed the same levels of access as USER1, all users could be added to a group (e.g., DBASEUSERS). The group DBASEUSERS could then be granted the same trustee rights as USER1.

The important distinction here is that Directory Rights take precedence over Trustee Rights. To continue with the previous example, if USER1 has Trustee Rights to the SYS:APPS\DBASE directory of R,O,S,C,M,D, but the directory SYS:APPS\DBASE has directory rights of R,O,S, the EFFECTIVE rights for USER1 are only R,O,S. USER1 can only read, open, and search for files in the SYS:APP\DBASE directory.

File Attributes. Directory and Trustee rights apply to all files in a given directory. File attributes can be assigned on a file-by-file basis and take precedence over directory rights and trustee assignments. File attributes are:

RO	Read Only
RW	Read/Write

S Shareable
N Non-Shareable

If a user has rights of Read, Open, Write, and Search, to the DBASE directory, but the file TEST.DBF has been assigned the attributes Sharable and Read Only, then USER1 cannot write to file TEST.DBF.

Security Equivalences. The Trustee Assignments of one user can be equated to another user by the Supervisor. The first user is said to be "Security Equivalent" to the second user. Any rights of the first user are given to the second user after the equivalence is made. Care must be taken when using this feature.

Supervisor Rights. The Supervisor has all rights to all directories on a given file server. Furthermore, an ID that has been set security equivalent to the Supervisor, also has all rights to all directories. NDPD LAN Operational Policy 310.09 mandates that only the System Administrator and backup System Administrator know passwords for the Supervisor ID or Supervisor-equivalent ID's. The number of Supervisor-equivalent ID's should be kept to an absolute minimum.

Details on all levels of security can be found in the NetWare Supervisor's Reference. Recommendations for use of file attributes in an application sharing environment can be found in the Application Operations Section of the LAN Technical Guidelines.

Rights should be granted on an as-needed basis. For example, do not assign Parental or Write rights for a user or group of users who only need Read access.

Regularly scheduled backups of file server data is essential for protection against catastrophic corruption or loss of data.

CABLING MAU'S AND WIRE CLOSETS

MAU's should be housed in a wiring closet with a lockable door. This door should remain locked at all times when the System Administrator does not need access.

LAN's used for processing Confidential Business Information should have unexposed cabling or controlled access to the facility where the cable is run.

On unused cable runs, patch cables should not run between the distribution rack and the MAU's

DIAL-IN ACCESS AND GATEWAYS

Phone numbers for dial-in access should be given out on a need-to-know basis.

Passwords must be used at the host PC (i.e., the PC on the LAN running NetWare AnyWare). When a user dials into the LAN from a remote PC, he must be forced to enter a password.

If available, the Gateway Dial-Back feature must be used. This feature, available with the Novell Asynchronous Communications Server (NACS), allows a remote user to call in. NACS then severs the connection and returns the user's call.

14. AUTOMAXX

OVERVIEW

AUTOMAXX is the DOS shell or user interface selected for use on EPA MS-DOS-based microcomputers and Local Area Networks (LAN's). It has been site-licensed by EPA and can be distributed throughout the Agency at no additional charge to the user.

Features of the AUTOMAXX system include:

1. User-defined menus which allow execution of one or more DOS commands with one keystroke. Up to 50 menu screens can be defined.

2. A PC-fixed disk manager with the following:

   DISPLAY of files and directories
   RENAMING of files and directories
   CREATION and REMOVAL of directories
   POINT AND SHOOT feature for running programs
   WHEREIS feature to find files anywhere on a disk
   File encryption/decryption

3. POP-UP Calendar and Calculator

4. PASSWORDS for menu selections

5. TIMED EXECUTION of menu options

6. Screen Saver

7. Keyboard Macros

8. File BROWSE capability

9. LINKS with any editor to view or edit files

10. Printer definition files

11. Disk FORMAT Recovery Software

Obtaining AUTOMAXX System and Documentation

AUTOMAXX system files and documentation can be obtained in one of three ways:

1. When ordering an Epson Equity III+ computer with a hard disk from Federal Data Corporation, AUTOMAXX is included with the computer.

2. When ordering a LAN file server from Systems Management American Corporation, AUTOMAXX is included with the file server.

3. AUTOMAXX files can be downloaded from the LANSYS Bulletin Board (LANBBS). The most current version of the standard batch files and menu definition file will always be available from LANBBS. Changes were made most recently to these files to incorporate new menu choices and to increase readability. All AUTOMAXX files are stored in archive format on the LANBBS. To obtain these files you must:

   - Log into the LANBBS with a valid USERID.
   - Download the AUTOMAXX files using a binary file transfer protocol (XMODEM or YMODEM).
   - Unarchive the files using PKXARC.COM. This program can also be downloaded from the LANBBS.

INSTALLATION

1. Installing AUTOMAXX on a workstation hard drive:

   If you purchased an Epson Equity III+ from FDC, then AUTOMAXX should already be installed for you. If not, proceed as follows:

   - Obtain the AUTOMAXX files.
   - Copy these files to the root directory of the workstation's hard disk.
   - Ensure that the PATH statement in the workstation's AUTOEXEC.BAT file includes the path for the root directory (e.g., C:\).

2. **Installing AUTOMAXX on a file server:**

   If you purchased a file server from Systems Management American Corporation, then AUTOMAXX should already be installed on that server. If not, proceed as follows:

   - Obtain the AUTOMAXX files.
   - Log in to the server using an ID with rights to the SYS:SUPER\AUTOMAXX directory. If this directory has not been created, you will need to do so.
   - Copy the AUTOMAXX files into the SYS:SUPER\-AUTOMAXX directory.
   - Ensure that all users have Read, Open, and Search rights to that directory.

     Note: Many LAN installations have AUTOMAXX installed on both the network file server and the workstation hard disks. The workstation is under control of the local copy of AUTOMAXX until the user logs into the network. At that point the file server copy of AUTOMAXX takes control. With this configuration, the user is allowed to switch back and forth between workstation and file server AUTOMAXX control. This allows the user to take advantage of both local and centralized resources. This configuration is highlighted in the OPERATION section.

OPERATION

As a menu, AUTOMAXX operates similarly to other menu systems in that initial execution and looping return to the menu is controlled via DOS batch file. The most simple form of a batch file used to control AUTOMAXX is as follows:

EXAMPLE: MENU.BAT

```
C:
CD \
AUTOMAXX /V=C:\VU.EXE/ M=C:\AUTOMAXX.DAT/E=C:\
```

```
/U=C:\
AUTOTEMP
```

When MENU.BAT is run, AUTOMAXX.EXE is executed. Note the parameters supplied to AUTOMAXX.EXE. An explanation for the use of these parameters can be found in the AUTOMAXX.DOC file. The /M parameter is explained below as an example.

When AUTOMAXX.EXE is executed, one of the routines it performs is to read the contents of AUTOMAXX.DAT into the workstation's memory. AUTOMAXX.DAT is the menu definition file created by the System Administrator. It contains the menu screen definitions and DOS commands which are executed when the user chooses a menu option. A sample portion of an AUTOMAXX.DAT file is shown in Figure 14-1.

A menu title or submenu is defined by a line preceded with a %. A menu option is defined by a line beginning with an *. All commands between two * commands are part of a menu option. The text following the * is displayed as a menu choice for the user. When the user selects a menu choice, all commands preceded by a + are written to a file called AUTOTEMP.BAT. After that point, AUTOMAXX.EXE stops executing, and control is returned to MENU.BAT where AUTOTEMP.BAT is executed. Note that the last + command for any menu option is always +MENU. Thus, the last command within AUTOTEMP.BAT always calls MENU.BAT and the cycle starts over again.

Explanations for all AUTOMAXX.DAT commands and all AUTOMAXX.EXE command line parameters can be found in the documentation AUTOMAXX.DOC.

Dual Installation - File Server and PC.

AUTOMAXX can be installed to allow both local operation and shared network operation. This is accomplished via enhancement of the MENU.BAT file. The copy of MENU.BAT stored in the root directory of the workstation (the LOCAL COPY) is modified to first verify that the user is logged into a file server. If so, the file server copy of AUTOMAXX is run. If the user is not logged into the file server, the workstation copy of AUTOMAXX is run. Figure 14-2 contains a listing of the most recent edition of MENU.BAT.

```
;*************************************************************************
;*************************SERVER BASED AUTOMAXX.DAT***********************
%FILE SERVER MENU
 *DATA BASE
    >DATA BASE SELECTION MENU

 *SPREAD SHEET
    >SPREAD SHEET SCREEN MENU

 *WORDPROCESSING
    >WORDPROCESSOR SELECTION MENU

 *COMMUNICATIONS
    >COMMUNICATIONS SELECTION MENU

*LOGOUT FROM NETWORK
 +ECHO OFF
 +MAP S16:=SYS:\SUPER\AUTOMAXX
 +LOGOFF
 +PAUSE
 +C:
 +MENU

*EXIT TO SERVER DOS
 +ECHO OFF
 +echo Exit from AUTOMAXX.  Type MENU to return.
 +HOME
;*************************************************************
%DATA BASE SELECTION MENU

*DBASE III
 ; ******************* DBASE III ****************************
 +ECHO OFF
 +IF NOT EXIST SYS:\APPS\DBASE\XDBASE.BAT GOTO NOTFOUND
 +REM ELSE
   +Z:\APPS\DBASE\XDBASE
   +GOTO EXIT

 +:NOTFOUND
  +ECHO *** ERROR *** DBASE III MISSING  (XDBASE.BAT) ***********
  +ECHO *** APPLICATION NOT INSTALLED ON THE FILE SERVER !
  +PAUSE

 +:EXIT
  +MENU
.
.
```

Figure 14-1. Sample AUTOMAXX.DAT File

MENU.BAT

```
ECHO OFF
rem ***************************************************************************
rem  *****If user is logged into network, execute a server based
rem  MENU**** IF EXIST Z:\PUBLIC\SYSCON.EXE GOTO SERVM
rem ************Else - execute local work station AUTOMAXX**********
:WSMENU
  IF NOT EXIST C:\AUTOMAXX.EXE GOTO ERR1
        C:
        CD\
     AUTOMAXX /V=C:\VU.EXE /M=C:\automaxx.dat /E=C:\ /U=C:\
AUTOTEMP

:SERVM
rem ***************************************************************************
rem ** The user may specify the name of a Novell menu definition
rem ** file.
rem ** If a .MNU file is entered as a parameter, call the Novell***
rem ** Menu System instead of AUTOMAXX - Else call AUTOMAXX.*******
  IF "%1" == "" GOTO FILESV
     IF NOT EXIST Z:\PUBLIC\NOVLMENU.* GOTO ERR2
     NOVLMENU %1
     GOTO EXIT

:FILESV
rem ***************************************************************************
rem **If the server based AUTOMAXX has already been called and
rem **the user* rem **has chosen the option - CALL WORK STATION
rem ** MENU, then the variable* rem **%WSMENU% gets set to rem 1.
IF "%WSMNU%" == "1" GOTO WSMENU
     IF NOT EXIST Z:\SUPER\AUTOMAXX\AUTOMAXX.EXE GOTO ERR3
        IF "%USERID%"=="SUPERVISOR" SET USERID=SUPER

rem ***************************************************************************
rem ** Copy the default printer definition file to the user's rem
**home directory if they do not already have one present ** IF NOT
EXIST F:\USER\%USERID%\AUTOMAXX.PDF COPY
Z:\SUPER\AUTOMAXX\AUTOMAXX.PDF F:\USER\%USERID%\*.*
rem ***************************************************************************
rem *Call AUTOMAXX /E=directory where automaxx support files are
rem found          /M=Path for AUTOMAXX.DAT- menu definition file
rem               /U=Path where AUTOTEMP.BAT is written
rem               /V=Path for default editor -VU.EXE
Z:\SUPER\AUTOMAXX\AUTOMAXX /E=Z:\SUPER\AUTOMAXX\
/M=Z:\SUPER\AUTOMAXX\AUTOMAXX.DAT /U=F:\USER\%USERID%\
/V=Z:\SUPER\AUTOMAXX\VU
```

Figure 14-2. MENU.BAT Listing (Page 1 of 2)

```
rem*****************************************************************
rem *******Run Batch File - AUTOTEMP.BAT created when the user
rem *******makes a menu choice.
*****************************************************************
F:\USER\%USERID%\AUTOTEMP
GOTO EXIT
rem ****************************ERROR ROUTINES*****************
:ERR1
ECHO * * *  ERROR - AUTOMAXX.EXE NOT INSTALLED ON LOCAL DRIVE  *
GOTO EXIT
:ERR2
ECHO * * *  ERROR - NOVELL MENU (NOVLMENU) MISSING  * * *
GOTO EXIT
:ERR3
ECHO * * *  ERROR - AUTOMAXX.EXE NOT INSTALLED ON FILE SERVER * *
:EXIT
```

Note the use of parameters on the AUTOMAXX command line which specify where the work files are to be placed. Essentially, on the network version, AUTOTEMP.BAT is written to each user's SYS:USER\<USERNAME> directory. Furthermore, the AUTOMAXX.DAT file is shared by all users and, is stored in the SYS:SUPER\AUTOMAXX directory.

Again, keep in mind that both the local and the file server copy of AUTOMAXX.DAT have options that allow the user to switch back and forth between the two.

Figure 14-2. MENU.BAT Listing (Page 2 of 2)

TROUBLE-SHOOTING

Configuration Errors

With the exception of those anomalies listed later in the section titled "Known Bugs", most problems encountered during the configuration and use of AUTOMAXX are caused by improper syntax:

AUTOMAXX.EXE command line parameters

AUTOMAXX.DAT menu definition syntax

DOS commands

AUTOMAXX.EXE COMMAND LINE PARAMETERS

By default, AUTOMAXX.EXE "expects" to operate in the root directory of the C: drive. It expects to find the AUTOMAXX.DAT, help files, and default editor there. It expects to write the temporary file, AUTOTEMP.BAT, there as well. If a user copies all AUTOMAXX files to a directory other than C:\ and attempts to run AUTOMAXX.EXE, he will receive an error message such as:

Could not open C:\AUTOMAXX.DAT - Press Esc.

AUTOMAXX does, however, allow the user to change the directories associated with these files through command line parameters. Use of these and other switches are explained in detail in the AUTOMAXX documentation, Pages 16 and 17.

AUTOMAXX.DAT MENU DEFINITION SYNTAX

The syntax used for definition of menus and the ordering of commands within the AUTOMAXX.DAT file is explicitly stated in the AUTOMAXX documentation, Pages 5 and 6. If a user deviates from the documented syntax when constructing the AUTOMAXX.-DAT file, the menu will not operate correctly. Typing errors are frequently the cause of AUTOMAXX malfunction. One common mistake is creating a submenu with the % command, but misspelling the title of that submenu within a > command. The menu loads but, when the user selects the choice for the improperly typed > command, the program does not execute the menu option.

DOS COMMAND SYTAX

Essentially, the same logic used to create DOS batch files is used to construct the logic carried out by an AUTOMAXX menu option. If an option fails during execution:

1. Note any returned error messages.

2. AUTOTEMP.BAT will contain the commands that you are trying to execute. Run AUTOTEMP outside of the AUTOMAXX menu. This will tell you whether the problem stems from the DOS batch commands or from the AUTOMAXX.DAT setup.

3. Run the commands from the menu option, one at a time, in order to isolate the command.

4. Ensure that drive letters, paths, search drives, and effective rights are set properly.

Known Bugs

Graphical Tree. AUTOMAXX has a feature which displays a graphical tree directory structure for a workstation hard disk. This feature, along with the feature that redraws the tree graph, will not function properly on a network drive. This problem will be corrected in the next release of AUTOMAXX.

WHEREIS Command. AUTOMAXX has a feature which allows the user to locate files on his workstation's hard disk. The user enters a file name or general filename (via use of wildcards, ? and *), and AUTOMAXX searches the disk's directory table for all occurrences of the name. This feature does not work reliably on a network disk; characters will be displayed and the workstation will lock up. This problem should be corrected in the next release of AUTOMAXX.

15. APPLICATIONS SOFTWARE MANAGEMENT AND MAINTENANCE

OVERVIEW

Software on the network falls into two categories: applications software and system software. Commercial applications software includes packages such as WordPerfect, LOTUS, dBASE, FOCUS, and SAS. User developed applications include programs written in programming environments such as dBASE III Plus. System software consists of the Novell NetWare file server operating system, workstation shell programs, and network menu and command line utilities. Users work directly with applications software, but do not have direct interaction with the network operating system or workstation shell programs except to assure they are loaded before attempting to log in to the file server. Network users do, however, need to understand the basics of using the AUTOMAXX menu and command line utilities.

The LAN Administrator is responsible for the installation and initialization of applications software and data bases, and for ensuring the integrity of applications sharing activities. Additionally, the LAN Administrator is responsible for ensuring that applications and system software perform as expected, that users have proper documentation and training in using the software, and that users have access to technical support for specific questions regarding the software.

Application Sharing

There are two categories of applications software on the network: single-user applications and multi-user applications. These are distinguished by how data files are used. If the data files are used by only one person at a time, the application is single-user. If more than one person uses the same data file at the same time, the application is multi-user.

Some vendors sell network specific versions of their software, but these are primarily single-user applications. For example, some word processors and spreadsheets are inherently single-user; only one user should be working with a single document or spreadsheet at a time. The difference between single-user and network specific versions of word processors and spreadsheets is that the

network specific versions usually include a section of code that is resident on the file server to control various user configurations and to perform the file server I/O. True multi-user applications, such as dBASE III Plus, execute on each user's workstation, but control simultaneous access to records in a data base stored on the file server through file and record locking processes.

Most of the single-user software packages recommended by the Agency will allow multiple users to execute the application simultaneously. It is, therefore, up to the user and the LAN Administrator to restrict access to data files used by these applications to a single user at a time.

The NetWare FLAG utility allows temporary restriction of file access for user applications. The FLAG utility can be executed via menu batch commands for each application, allowing the file locking procedures to be transparent to the user. Files are normally created as Non-Shareable/Read-Write. If they are to be shared, FLAG is needed. If not, the protection is there by default. More information regarding the use of the FLAG command can be found in the Netware Command Line Utilities Manual.

Distribution of Manuals

An important issue, often overlooked during LAN implementation, is the availability of adequate documentation for using applications software and network utility programs. It is of special interest to the LAN Administrator to ensure that access to appropriate documentation is available to all users. Otherwise, undue time will be spent by the Administrator answering questions from the user community.

All single-user application packages are sold with only one copy of documentation, while some multi-user application packages are sold with several copies of documentation. The Novell NetWare documentation contains only one copy of each manual per installation, although some software vendors do allow the purchase of multiple copies of their documentation. Many facilities create a library for applications and NetWare documentation, providing all users with common access. If needed, and if the vendor complies, multiple copies of documentation for specific applications can be purchased. Depending on the number of users, multiple copies can either be distributed or stored in the common library.

User Training

There are two areas of concern to the LAN Administrator regarding user training. First, users must be competent in the use of the network menu system, AUTOMAXX menu utilities, and NetWare command line utilities. Second, users must be aware of the differences in running single-user or multi-user applications on the network.

It is obvious that the LAN Administrator will be asked, from time to time, for help on specific problems. However, a great many of the "start-up" problems inherent to new network users can be overcome by demonstrating the use of the network in a class environment.

Because of the number of issues involved in networking, it is best not to cover all aspects of using the network in a single class. Instead, a separate 1- or 2-hour class should be devoted to each topic.

Possible topics for separate classes include:

- Signing on and using the AUTOMAXX menu utility
- Printer functioning and maintenance
- NetWare command line utilities
- AUTOMAXX menu utilities
- Managing public and private data files
- Communication gateway functioning and management
- Use of specific applications software on the network

Additionally, copies of this guide could be distributed to each network user. Though much of this guide contains information not relevant to daily use of the network, users will benefit by having access to the information.

INSTALLATION

Application Loading and Installation

The focus of work on either a single-user workstation or a network is the use of application software. It is the job of the network Supervisor to load application software, configure and initialize the software, and ensure that the users have appropriate access to the software. Network users will, for the most part, presume that application software being used on the network will perform in a manner similar to that of software on a standalone

workstation. Because of the use of applications that have been developed using an application programming language, as in dBASE, such uses will be referred to as dBASE applications. This will differentiate the applications from standard application programs, such as LOTUS, WordPerfect, and dBASE.

Differences in single usage versus network usage of any particular application software program should be documented and, if necessary, users should be trained in the use of applications on the network. Additionally, the network Supervisor should be responsible for ensuring that application software copyright or licensing agreements are not violated by multiple users accessing a single copy of certain software. Benefits of using application software on a network include sharing of data files, documentation, and system resources, such as printers. It is the Supervisor's responsibility to ensure that multi-user data files and shared printers and other resources can be properly accessed by all network application software packages.

Installation of Software on Server and Workstations

After directories, users, passwords, and rights have been defined, the application files you plan to use (word processors, spreadsheet programs, etc.) must be loaded into the appropriate directories. File rights, if necessary, should be established. On a file server, applications should generally be installed in a subdirectory of the SYS:APPS directory. Issues of concern to the network Supervisor include:

- Vendor and publisher agreements that pertain to the number of users accessing an application program simultaneously.
- Whether or not the application software is designed to be used in a multi-user environment.
- Actual installation and configuration of application software on the file server.
- Modification of multi-user software file rights to allow application files to be shared.

When installing an application program on the server, ensure that no other users are on the network. Because the proper installa-

tion of application programs is a critical step, it is best not to have other users accessing the file server, adding unnecessary complications. The LAN Administrator must establish a software install and upgrade procedure that will minimize interference with normal network use.

For example, while installing a new version of an accounting system, other network users are using the old version of that software during the install procedure. Data could be lost due to copying new configuration files during the installation.

There are basically two procedures for loading software onto a file server. Some applications either require or suggest the use of a provided "install" utility. This "install" program will typically perform functions such as creating the necessary directories, copying the appropriate files to the directories, and performing some application configuration. Other application packages require that programs on the distribution diskette(s) be copied to the appropriate directories on the hard disk (file server).

Before attempting to load an application program on a file server, read the program's documentation. Typically, a section is provided explicitly for installing software on a hard disk and/or network. Also, the documentation may indicate whether or not the program files need to be loaded into a specific directory. Most applications that do require specific directories will also provide an "install" utility to help ensure that the appropriate directories are created and files are loaded in the correct hard disk directories. Programs such as WordStar, WordPerfect, MultiMate, DisplayWrite IV, LOTUS, and dBASE III Plus, do not require that the program files reside in any specific directory.

To load an application on the file server, perform the following steps:

1. Log in to the network as the user Supervisor, or as a user with appropriate directory trustee rights.

2. Change to the appropriate directory, using the DOS command "CD \directory_name". This directory should already exist on the file server. If not, create the directory under the SYS:-APPS directory.

For programs without auto-install procedures:

3. Insert the first program disk in floppy Drive A: and type the DOS command "COPY A:*.*". This will copy all of the files from the floppy to the currently logged file server directory.

4. Repeat step 3 for each program distribution diskette.

For programs with auto-install procedures:

3. The program documentation should indicate the name of the program to run to initiate loading the application on the hard disk. Typical install program names are "INSTALL" or "HINSTALL". Not all programs on the distribution diskettes named "INSTALL" will actually copy the files; certain applications have "INSTALL" programs intended for configuration of the application after it has been copied to the hard disk. Some install programs require that the logged drive be changed to a floppy diskette, while other programs require that the hard disk be the currently logged drive. Additionally, some install programs will require command line parameters, typically to indicate the target drive for installation. An example of this might be: "A:INSTALL C". Also, certain install programs, when executed will prompt for the target drive and directory.

Generally, most install programs will simply copy the appropriate files to the hard disk. When required, the install program will prompt you to insert the appropriate distribution diskettes in the floppy drive to complete copying of files to the hard disk.

Initial Application Configuration

Most application programs, when first loaded to a hard disk, require that a configuration program be run prior to actually executing the application. The programs mentioned in this document (word processing, spreadsheet, and data base management) all have different configuration needs. Refer to the program's installation documentation for the name and instructions for the Configure program.

WORD PROCESSORS

Word processors typically need to be informed of the types of available printers. Some word processors allow for multiple printers to be configured for an application, and the user can select among those available at print time. Other word processors allow specification of the default document directories. For use on a network, when default directories are required, public directories are the easiest for maintaining document storage compatibility among users. Certain word processors include utility programs that will perform specific tasks, such as speeding up the keyboard, however some of these programs hinder proper functioning of the word processor over the network. For example, MultiMate Advantage is shipped with the keyboard speedup enabled. You must change this default when using the network.

SPREADSHEETS

LOTUS, as well as other spreadsheet programs, requires that a configuration program be run prior to executing the application. The most important function of LOTUS' configuration program is to install the correct screen drivers for use with the application. This means that if monochrome and color graphics adapters are on different workstations, multiple copies of the LOTUS program or set-up files may need to be loaded onto the file server to accommodate the needs of different workstation displays and display adapters. If this is done, each workstation can access separate copies of the program configured specifically for the appropriate workstation display type.

Obviously, loading multiple copies of software is more costly and takes up valuable disk space. When an application allows, create multiple versions of configuration or set-up files with different names. When and application is to be loaded, copy the appropriate configuration or set-up file to the valid name expected by the application using DOS batch files. The standard EPA menu system provides an example of application batch file execution.

DATA BASE MANAGEMENT SYSTEMS

dBASE requires no special configuration. However, before the program can be executed, a program called "ID" must be executed. On the first copy of dBASE, enter the owner as EPA. This program will also prompt for the serial number of the distribution diskettes. Existing Agency copies can be used; simply load the software on the file server and enter the existing serial number. This procedure ensures that you have purchased original copies of the distribution diskettes, and configures the program to indicate the owner of the application. These copies should not be used on other PC's. Other data base management programs may have separate Configure utilities that require more specific information regarding program file directories. Consult the installation documentation for the application program you have loaded on the file server for detailed instructions.

Program Initialization

In addition to running a Configure program prior to executing an application, many packages have "set-up" options which allow the specification of certain default parameters that pertain to normal program usage. These parameters are loaded as the current parameters each time the application is executed. Applications that do not have particular menu items specified for "setup" often have default selection procedures built into different program aspects. A general discussion of the initialization procedures for each of the three types of applications covered in this document - word processors, spreadsheets, and data base managers - are described below.

WORD PROCESSORS

The most prevalent default configuration option specified for word processing programs is the printer type. A separate "printer install" program is included for some applications; for others, the printer is defined during the initial configuration program, or options may be built into the program to allow specification of the current default printer(s). Depending on your word processor, one or more printers may be selected from a list of available printer drivers to be used as the default printer configuration. Only one printer can be specified at a time to be the current printer for any program, though additional printers may be

specified as alternate printers with some word processors. Other parameters that may be available for printer configurations include:

- Page length
- Top and bottom margins
- Page number type and positions
- Justification
- Widows (minimum number of lines from a paragraph allowed at the top of a page)
- Orphans (minimum number of lines from a paragraph allowed at the bottom of a page)

Additionally, some word processors allow the page format and other command keyboard sequences to be defined by the user. If a standard set of keyboard command sequences has been specified for use on your network, these keyboard sequences should be configured prior to network use of the program. If current documents, boilerplates, or style sheets are needed for use on the network, they should be loaded into the appropriate shared, public, or private directories.

SPREADSHEETS

LOTUS and other spreadsheets require little printer configuration; they are designed to work with most printers. Any printer control sequences necessary for print formatting are entered in the Printer Set-up menu options. Most of the other global configuration options are set to valid default values upon initial program execution.

Users with Write Access to the spreadsheet program directory can update the default printer set-up control sequences at any time. As different network printers are specified on the file server, the network Supervisor or network users may need to specify different printer set-up control sequences. Program and configuration files can be protected against corruption by use of the FLAG utility. As with word processors, if worksheet data files currently exist that will be used on the network, they should be loaded into the appropriate shared, public, or private server subdirectories. The FLAG command can be used on files in public or shared direc-

tories to protect against multiple concurrent accesses of the same file.

DATA BASE MANAGEMENT SYSTEMS

dBASE III Plus requires no menu configuration for the default printer, directories, or other parameters. Unlike most word processors and spreadsheets, dBASE can be driven by either a menu, via the Assist function, or by typing commands at the "dot" prompt on the command line.

The default configuration that is used when the program is initially loaded into memory is read from a file called "CONFIG.DB" in the current directory. This file contains information used by dBASE and indicates the default values for parameters, such as the program editor to be used, the state of the status and indicator lines, the state of the application generator, and various other data. A complete description of the options available to be included in the "CONFIG.DB" file can be found in the dBASE III Reference Manual. Other options, such as output routing, can be specified by typing a command sequence (e.g., the SET ALTERNATE command at the dot prompt) while the program is running.

If dBASE applications are to be loaded on the file server, they should be copied into the appropriate public directories. Read the application documentation for information regarding whether directory location of applications can be configured from within the application program, or whether the application will assume that both the dBASE program and the application program files must co-exist in the same directory.

Many dBASE application programs require that default directories for data files be designated, and that the data bases for the application be initialized prior to using the application. Consult the dBASE application documentation for specific directions for initializing data bases.

Of primary concern when running dBASE applications on a network is whether the application itself was written intentionally to run on a network. dBASE III Plus includes commands in its programming language designed to provide record LOCKing and UNLOCKing functions. Any dBASE application program written

prior to the introduction of dBASE III Plus could not be written specifically for network usage. If the application programs allow modification of the source code, record locking can be added to them. Use of data base applications, or any data base in command mode under dBASE, that do not use record locking should be governed cautiously. Simultaneous record updates by multiple users, or modification of data base structures, can quite easily result in a corrupted data base. Additional information for application developers is available in the Application Engineering Guide.

Vendor and Publisher Agreements

Software vendors wish to protect their investment in developing application software. This is accomplished by imposing either physical or legal methods which require that their software be used as intended. The physical method of protection is known as copy protection. Two legal methods of protection are license agreements and copyright laws. One additional type of vendor-user arrangement that has become prevalent is the "shareware." Though not as strict as licenses, shareware software and some public domain software generally requires that users pay a small registration fee in order to obtain software upgrades and support from the vendor.

COPY PROTECTION

The use of copy protection in the MS-DOS area has been declining; most of the best selling MS-DOS software packages are not copy-protected. Some methods of software copy protection and their use in a network environment are described below. In general, it is best to avoid copy-protected software altogether; unnecessary problems often result from its uses, especially in a network environment. However, in some situations, suitable non-protected software may not be available, and use of copy-protected software may be unavoidable.

KEY DISK SCHEMES

Some copy-protected software allows the software to be loaded onto a hard disk, even a network file server; but requires insertion of a "key disk" in the local floppy drive before the application will

run. Since the "key disk" cannot be copied, only one user can run the software at a time. Some vendors may allow users to purchase additional "key disks," allowing multiple users to run the software simultaneously. Generally, vendors will supply additional "key disks" only if they agree to have their software used over the network. Otherwise, entire packages have to be purchased for each user, or the key disk(s) must be passed around.

HARD DISK PROTECTION SCHEMES

As hard disks became more popular, users complained about the use of "key disks" in running applications. Vendors began to use a form of copy protection that loaded the application software onto a hard disk and did not require the use of "key disks." Such protection methods generally employ some form of physical protection related to the structure of the hard disk media. These protection methods use low level details about the hard disk organization that may not be duplicated on a file server. For example, the protection scheme may directly access the hard disk controller, bypassing the operating system and not allowing the NetBIOS software to work correctly; or it may depend on the exact placement of the protected programs on the hard disk, which would be endangered if the file server were backed up and later restored. Because of this, use of software that employs this type of copy protection is strongly discouraged. Some software in this category may function properly on a network; however, a burden still exists on the network Supervisor to enforce the single user, single machine license restriction. If it is necessary to attempt installation of copy-protected software on a file server, it is always best to do so before other applications have been loaded and prior to data base initialization or other network usage. Special care must be taken when backing up a server containing this type of software.

SITE LICENSE AGREEMENTS

License agreements from software distributors range from the simple to the very complex. Several large businesses and agencies have been successfully sued for failure to comply with these

license agreements. It is, therefore, critical that you understand the exact nature of licensing for the particular software you use.

Application Sharing Concerns

Most application software currently available was designed to run on single user applications. Some software vendors have either rewritten their software to run on networks, or have special versions available for network use. However, since network hardware was developed before network application software, the network operating system software was designed to allow most existing PC/MS-DOS software packages to be adapted to network use without modifications. Several items must be taken into consideration when attempting to adapt single-user application software to run under the NetWare operating system. These include:

- Copy protection (including LOTUS, Versions 1 and 2
- Simultaneous file updates
- Disk accesses
- Printer and resource sharing

Several problems exist when attempting to run a single user application on a network. They are:

- Concurrent access and update to data files
- Sequential program configuration or profile updates
- Application temporary file information updates

The first problem involves updating a data file that two or more users are working on simultaneously. If the application program was not designed for multiple users, changes made by one user can be lost if the file is later written to disk by another user. The typical scenario might be: User 1 and user 2 both load an application program; both also load the same data file or document. User 1 makes changes to the file and writes it to disk. User 2 makes changes to his copy of the original file and later

writes it to disk, overwriting the file modified by User 1. User 1's changes are lost.

The solution to this problem in a networking involvement center around organization. When files are to be shared by single user applications, communication between users about current work files becomes critical. The use of the FLAG facility to make data files Non-Shareable is crucial.

The second problem involves application programs that load configuration files upon initiation. For example, a program may behave differently if configured with a monochrome versus color monitor. Some applications allow users to configure default parameters or user profiles that will be in effect upon subsequent loads of the program. There are three ways to handle this situation. First, if the applications allow specifying different configuration or profile file names, then each user can set up a separate configuration or profile file in the application directory and load the configuration file when the program is up and running. Second, if the application will load and run successfully if executed from a directory other than the application directory, then each user may be able to save the default configuration or profile file in a working subdirectory. When the application is loaded, the configuration file is read from the current directory. Third, each user can be provided with his or her own copy of the software in a private network directory. The third method is discouraged; it may not be possible due to licensing restrictions, and it will consume extra file server disk space.

The third problem exists with certain application programs that write temporary files to disk during execution of the program. If two or more users are accessing this type of application simultaneously, then one user's temporary file can become corrupted by another user. Two possible solutions to this problem are:

1. If the application allows specification of data file directories, then each user can specify different directories after the program is loaded (or in the configuration parameters as discussed previously).

2. Access to the program can be restricted to one user at a time.

If you are unsure whether or not a particular application program writes information to disk during execution, conduct an experiment by loading the application into a read-only or write-protected subdirectory on the file server and then run the application. If the program functions properly, it does not need to write to the disk and can be shared over the network among multiple users, within license and copyright provisions.

If the suggestions above fail to solve multi-user access for a particular application, the problem can usually be avoided by loading separate copies of the application on the user's workstation disk drive. This is not recommended for most applications. If licensing and technical issues can be resolved, having one copy of an application on the file server is the preferred method because less disk space is consumed by the application and maintaining application revisions and updates is less complicated.

OPERATION

Application Administration

The primary daily task of the LAN Administrator is to ensure that the programs work as expected. In this regard, the LAN Administrator should verify each of the items in the following checklist on a regular basis.

- Menu choices should work as expected; applications should load properly and, when exited, the network menu should reappear.
- Menu choices that invoke applications with copy counters should be tested on multiple workstations to confirm that the menu script works as expected.
- Applications that are not on the network menu should load and work as expected.
- Applications that load by executing the FLAG command for program and/or data file security should be tested by attempting simultaneous access. The second workstation attempting access should receive a message indicating the status of the files.

- Applications that share data files (true multi-user programs) should be tested to confirm data integrity during multiple access of the same data file and/or records. If any problems exist, the program's configuration should be checked.

When removing applications from the network, the following checklist should be used:

- All program and data files should be backed up to tape.

- The program and data files (if appropriate) should be deleted from the file server.

- The directories for the applications should be removed from the file server using the DOS "RMDIR dirname" command.

- The MENU script file should be edited to reflect the removed application.

- Trustee rights and security equivalences for the applications directories should be deleted or edited to reflect the change.

- Drive and Search mappings should be edited in both the System Login Script and User Login Scripts (the Script.Log include file) to reflect the removed application.

- Standard logins should be tested to confirm that drive/search mappings, directories, group and trustee security, and the network menu function as expected.

Any application that is intended for use by non-Supervisor, network users should be given access through the AUTOMAXX menu program. Section 14, AUTOMAXX, of this guideline discusses the use of the AUTOMAXX menu program to automate loading of applications. Additionally, the sample portion of the AUTOMAXX.DAT file, along with AUTOMAXX documentation, should be used as a reference for modification that may be needed to the AUTOMAXX.DAT file supplied by SMA.

The LAN Administrator must be cognizant of licensing agreements on specific software. For example, if three copies of LOTUS have been purchased by your work group, then the AUTOMAXX.DAT script should ensure that only three copies of LOTUS are in use simultaneously by network users.

If personal programs or other applications exist that should not be listed on the network menu system, the LAN Administrator should install the programs in appropriate directories and train users in using the programs from the DOS command line prompt. Access can be restricted by adding individual or group trustee rights for the appropriate users. If applications exist on the menu system, but restricted access to these programs is desired, the LAN Administrator can create a special group allowing access rights to the applications directories and adding the appropriate users as members of that group.

Production Control

A "job" in this discussion is meant to indicate any program execution submitted by a user. There are two classifications for identifying jobs on the network. First, jobs can be classified as production work or development work. Second, jobs can be classified according to the type of resources they use. The resource tasks used by jobs can be further defined as being compute intensive, disk intensive, and print (or other I/O) intensive.

Most network jobs are classified as production. Development jobs are part of the process of testing out programs and data sets, correcting problems, and resubmitting jobs until they work as desired. Development jobs are usually performed during the normal work day. If possible, development work can occur outside of production work hours. However, the LAN Administrator should be prepared to compromise network resources during the Development phases of tasks.

Production jobs should be monitored by the LAN Administrator for possible network resource competition. If a single production job tends to take over the file server, or if the printer is tied up for one or more hours, the rest of the network suffers. A solution to large production jobs is to schedule them, if possible, to run at the end of normal working hours, on weekends, or during designated hours on designated days.

Software Upgrades

All commercial applications software and network software should be registered with the vendor as soon as it is verified that the software functions properly. Vendors will then inform registered owners of any upgrades available. When notices concerning upgrades for software are received, the LAN Administrator should review the enhanced functionality gained by ordering the upgrade. If the enhancements are of value to network users, the upgrade should be ordered and installed on the network. If the enhancements are not pertinent for your installation, the LAN Administrator may choose to wait for future upgrades. However, it is best to maintain the latest version of software whenever possible. If technical support from the vendor is requested, the vendor will generally assume that you are working with the latest version.

Compatibility with other users is another reason to maintain the latest version of software. When data needs to be exchanged, it is safe to presume that other users will also be maintaining the latest version of software.

Another reason to keep your software upgraded is that upgrading beyond single increments in software versions is very difficult. If you skip minor release upgrades and later decide to upgrade for a major software release, the technical difficulties may be greater than they would have been if the software had been kept upgraded.

Installation of Software Upgrades

Software upgrades for network use fall into several classifications. They include:

- Operating system upgrades.
- Server-based applications, which can be either single - user upgrades or multi-user (LAN) upgrades.
- Workstation-based applications upgrades.

The following checklist should serve as a guide when making server-based software upgrades:

- Always make an archive tape backup of the old software and data files associated with the software before upgrading.

- Ensure that all users have logged off the file server before beginning the upgrade procedures.
- Most software packages contain an install utility or instructions for performing upgrades from previous to current releases. Always follow the install instructions carefully.
- If upgrading from single-user to multi-user versions of software, check whether a conversion needs to be run on the application's data files. If so, proceed according to instructions.
- If upgrading operating system software, verify that all operations perform as expected after the file server has been rebooted.

If upgrading applications software, check that the software performs as expected. Check that the network menu works properly; some software upgrades may involve name changes for the executable files.

Software upgrades for programs that reside on workstations should always be performed when the workstation is in stand-alone mode (i.e., not logged into the file server). Information about upgrading EPA-developed custom applications can be obtained by contracting support personnel at NDPD.

Printer Sharing with Network Applications

Spooling is the method by which multiple print jobs can be submitted to a shared network printer. As each job is submitted, it is placed in a queue. Print jobs can be added and removed from the queue, and the print job's priority can be changed. Novell provides "CAPTURE," a resident program which intercepts normal printer output from programs and routes it to the network printer. Routing stops when the "ENDCAP" command is issued, or a timeout value, specified as a parameter with the CAPTURE command, is exceeded. Most applications, whether shared or not, will work with the network print method described previously. Problem which can occur, depending on how the application communicates with the printer, include the following:

- Direct hardware access by the application. (Uses non-standard DOS print functions).

- Network software filtering of control codes. (Application print formatting commands are not passed by the NetWare print facilities).

- Network software interjection of control codes. (NetWare printer commands conflict with the application formatting commands).

- Conflict between the network and application print buffering. (An application that uses non-standard DOS functions to buffer output may conflict with the NetWare spooler.)

- Non-release of shared printers by the application. (An application does not issue the ENDCAP command necessary to release the spooler for subsequent print jobs.)

- Setting of printer parameters by different applications. (One user sets the printer to condensed print, does not reset the printer at the end of the job, and the next user's memo is printed in condensed instead of normal type).

- Novell NetWare provides sharing of printers connected to the file server. There can only be up to two serial ports and three parallel ports. These printers are known to the operating system as COM1: and COM2: and LPT1: through LPT3:. PC/MS-DOS also recognizes the PRN: syntax as the default print device. NetWare redirects print output from an application by routing the output through the spooler and to the appropriate printer port. The default printer port is generally configured in the System Login Script or User Login Script; but output can also be routed by a user to another printer port with the use of the CAPTURE command. (Refer to the NetWare Command Line Utilities Manual.)

DIRECT HARDWARE ACCESS

Most application programs will send output directly by a C/-MS-DOS call to the PRN: or LPTx: device. Some application programs send output to the print device by accessing the printer via low-level BIOS system calls. NetWare is capable of intercepting these low level calls and routing them to the appropriate printer. However, if an application directly accesses printer port hardware on a local workstation, there is little that can be done to direct that application to use a network printer. Typically, applications access local hardware printer ports when configured to work with serial printers (COM1:...COM2:), but use standard MS-DOS or IOS interface calls when configured to work with parallel printers. Even if a serial printer is designated as the current printer on the file server, it is possible to print the application by configuring for a parallel printer and reassigning the printer port of the NetWare CAPTURE command. (Refer to the NetWare Command Line Utilities manual.)

APPLICATION BUFFERING

Occasionally, an application software program will have its own print spooler. For example, many word processors will buffer output while allowing the user to continue editing a document. These programs will sometimes check the hardware directly for printer status information that is not available from MS-DOS or BIOS. If the application allows disabling the print spooler (or print buffer), doing so may alleviate any possible problems. Network printers are controlled by the NetWare print services program, so buffered printing is automatic when printing on networked printers. Some applications allow printing to either a printer or a file. If you are having trouble printing to a printer, try printing to a file and then copying the printed file to the network printer. After the application has printed to a file, this can be done by typing: 'NPRINT file_name', or by issuing the 'COPY file_name LPT1:' command. Preferably, users can use the NetWare CAPTURE command to send files directly to the network spooler by typing: 'CAPTURE Q=queue_name.' (Refer to the NetWare Command Line Utilities manual).

NETWORK FILTERING OF CONTROL CODES

If an application program sends control codes to a printer in order to perform special functions, some of these codes may have special significance to the NetWare queue facility. This occurs most frequently when attempting to print graphics images or use special printer functions (such as microspacing, superscript, or subscript) on a network printer. Graphics images and special printer functions send a variety of control codes, and it is possible that strange effects may occur if specific character sequences are sent to a network printer. If you experience problems, try the print commands on a local printer attached to a workstation. If the printing works correctly, then the problem is likely to be control code interference over the network. NetWare performs little print command filtering and this type of problem should be minimal, if at all. However, several command sequences do control the queue parameters for networked printers.

NETWARE FORMATTING CONFLICTS

An additional problem can occur when a print job is not formatted correctly. This can be caused by unmatched print parameters between the NetWare CAPTURE facility, the network printer settings, and the application program settings for printing. Most application programs will attempt to control the print output format internally; therefore, the easiest solution is to reset the network printer to default configuration parameters, such as single space, page length, etc. If problems still persist, the application program print parameters can be adjusted to accommodate the network printer's settings. Typical parameters that can cause problems if settings are in conflict include:

- Page length (66 lines for an 11-inch page is standard).
- Line length (80 character lines are standard).
- Margins, Borders, and Page Offset. (The printer and spooler should be set to the physical limits of the paper being used (top and bottom margins of 0, left and right borders of 0, and page offset of 0.)
- Application conflict in printer parameter setting.

A major concern when using shared network printers is an application's use of special printer functions. Many application programs, such as word processors, will send the printer special codes for boldface, condensed print, or other features. Once a special mode has been set, most printers will remain in that mode until either explicitly reset with another control code or physically reset by turning the printer off and back on. When an application does not reset special printer functions, another user may attempt to print and find that the output is not formatted correctly. While this is true for standalone computers, it is more of a problem in a network environment.

Word processor applications frequently use special printer commands. Spreadsheet programs, like LOTUS, will also allow users to send special printer commands, such as condensed print, in order to print more information on a page. Data base programs, such as dBASE III Plus, allow special printer control commands, but these are seldom used in data base applications. Most application programs will send a minimum of print formatting commands to printers. In order to accommodate different types of printers, most applications contain a Configure utility or menu which allows the selection of the type of printer currently being used. If a network server has several different types of printers attached, then many of the application programs may need to be reconfigured to operate correctly with the appropriate current printer. Some users may also be able to temporarily route print output to alternate printers with the CAPTURE facility. The AUTOMAXX menu facility may include an option for the user to specify that the CAPTURE output be routed to any of the attached network printers. The CAPTURED output can then be reassigned from the AUTOMAXX menu.

- **Printer Use and Maintenance**

Printers will regularly run out of paper. Laser printers require special consideration because of the small amount of paper typically allowed in the input paper tray. Laser printers have an additional problem in that the output tray also has a limited capacity. Paper jams can occur in any type of printer, and ribbons or toner cartridges require regular replacement. When using local printers, it is obvious when one or more of these problems occur. But, on a network, problems can exist for a long time before users become aware of them. The NetWare PCONSOLE facility display indicates which print job(s) are in progress

and which jobs are in queue. If, by examining the display, it appears that any one job is taking too long to print, then printer problems may be suspect. Information on using the PCONSOLE utility can be found in the Netware Supervisor's Reference Manual.

Printing With Application Software

There are three primary classifications of software that will be loaded on a network file server. They are word processors, spreadsheets, and data base management systems. Additionally, data base management system applications, such as the CERCLIS WasteLAN program, may be loaded on the network file server.

WORK PROCESSORS

One of the most common uses of personal computers is word processing. It is rare when more than one person needs to update the same file at the same time. If it is possible for more that one person to access a document simultaneously, the document can be protected against corruption by using the NetWare FLAG facility. For this reason, the use of single-user word processors on a network should present no problems. The network file server should be used to store the program files for the word processor and the document files created by each user. The placement of the program files may be dictated by the application program itself, but more likely the location can be determined by the server directory structure designed by the network Supervisor. Document files should be stored either in user private directories on the network, in shared data directories on the network, or on the user's personal system. If multiple users will be using documents stored in public directories, the documents can be protected by using the NetWare FLAG command. If the FLAG command is executed with Non-Shareable Read-Write (NSRW) prior to working with a document, the first user will have normal access to the document, but subsequent attempted accesses by other users will receive a NetWare message indicating the file is in use. After the original user finishes with the file, another user can access it.

Several different word processors are available to run on the Novell network. Those available on the EPA SMA contract are: WordStar (MicroPro), WordPerfect (WordPerfect Corporation),

MultiMate (Ashton-Tate), DisplayWrite 4 (IBM), and Lexitype Plus. These word processors are supported by EPA.

Some word processors make use of style sheets, or boilerplates, when preparing documents in a common format. If available, style sheets should be placed in common or shared directories so that different users can have access to them. This will enforce more consistency among users. Quite often, users will store documents in private directories while working with them. When the documents are completed, they can be placed in a common or shared directory for final review by the appropriate users.

SPREADSHEETS

The Agency standard for spreadsheet use is LOTUS 1-2-3 (Lotus Development Corporation). The LOTUS program files should be loaded in the LOTUS directory, and worksheet files should be stored in separate, private or public data directories or on the user's personal system.

A spreadsheet program is used on a network in a manner similar to that of word processors. Individual users may prepare worksheets in private or public subdirectories, and then share the worksheets with other users by placing them in shared directories. Shared directories will allow commonly used spreadsheet templates and macros to be available to other users, saving these users a lot of time by providing access to commonly used functions. More and more frequently, applications are allowing the incorporation of LOTUS worksheet data directly or through special DIF files. Sharing data between applications is made easier by storing such data in shared or public directories.

DATA BASE MANAGEMENT SYSTEMS

The most popular data base application development system available on microcomputers is dBASE (Ashton-Tate). Many single-user Agency applications have been developed to run under dBASE. Beginning with dBASE III Plus, special distribution diskettes (the Administrator diskettes) are provided by the vendor to allow use of dBASE on a network. dBASE III Plus allows multi-user access, including updates to data files with record

locking, across a network. If a dBASE application is being developed internally, then the application developer can stipulate, either through configuration options or by direct coding to which directories the developed program code, application programs, and data files are to be stored.

EPA requires that if the dBASE application was developed outside of your installation, the application must allow that the application program files and data base files be stored in directories separate from the dBASE program itself.

Application Program and Data File Security

After all application programs have been loaded, configured, and initialized, file security for shareable and non-shareable files should be established. The NetWare FLAG command provides a means by which attributes can be specified for individual files or entire directories. A complete description of the FLAG command can be found in the NetWare User Reference, Part III: Command Line Utilities manual. Use the FLAG utility with caution and never change a file's attributes while another user is using the file.

Parameters available for use on files or directories with the FLAG command include the following: (Letters in brackets indicate acceptable abbreviations for the command parameters.)

- [N] NORMAL. File attributes will be Non-Shareable, Read/Write. These are the default attributes of a network file. This is the default security.
- [S] SHAREABLE. More than one user may access the file at a time.
- [NS] NON-SHAREABLE. Only one user may access the file at a time. (Default implied by [N])
- [RW] READ/WRITE. Users may read the file and write to or modify the file. (Default implied by [N]; exclusive from [RO])
- [RO] READ/ONLY. Users may only read the file; they cannot modify it. (Exclusive from [RW])

Examples of these commands are:

- **FLAG /LOTUS/*.* SRO.** Makes all files in the /LOTUS directory shareable and read-only.

- **FLAG /PROJECT1/*.* N.** Makes all files in the /PROJECT1 directory non-shareable, with read-write access. Note that if a user's Effective Rights do not allow access to a directory, then the file's attributes will not have any significance for that user. However, if a user does have complete rights to files in a directory, the file's attributes will take precedence over the user's Effective Rights.

VERIFICATION OF OPERATION OF APPLICATION

After all application programs have been loaded, configured, and initialized, and after the appropriate file attributes have been specified, a systematic check of application program functions and resource access should be made prior to general use of the applications by network users.

The steps involved in verifying proper application and printer access functioning are somewhat tedious, but do not require a great deal of time and effort, especially when compared to the time, effort, and frustration that can result from tracking an application problem once users are using the network. The procedures for checking program functions for each of the three types of applications described in this document are summarized below. For verification of multi-user file access, it is easier if you obtain the help of a co-worker so that each can us a workstation and any error messages can be reported.

Word Processing and Spreadsheets

1. Log on each successive workstation as a different user.

2. At each workstation, and under each user's logon name, load the word processing program. If many users are on the user list, then one user login from each user group would be a sufficient test.

3. Create a simple document for testing purposes.

4. Save the test document in each of the public, shared, and private directories available on the network. Ensure that the document saves correctly in the directories to which that user has appropriate rights, and that the document is not saved in the directories for which that user does not have write access.

5. Print the sample document to the default network printer and to a local printer, if available.

6. If more than one printer is attached to the file server, use the CAPTURE command to change the default network printer, or reroute printer output to one of the alternate printers. Print the sample document on each of the alternate network printers.

7. Repeat Steps 1 through 6 for each workstation and user (or user login from each user group) with access to the network.

8. Use the FLAG command on a file to provide non-shareable Read-Write security (e.g. "FLAG file_name.txt NSRW"). Have users at two workstations attempt to access the FLAG'd file concurrently. NetWare should provide the second user with an error message.

If any problems are diagnosed, use the guidelines outlined above, consult the program's documentation to correct the problem, and attempt the file or resource access again. Repeat these procedures until all file, printer, or other resource accesses work as expected. If you cannot resolve a problem, contact NCC User Support.

Data Base Management Systems

1. Log on each successive workstation as a different user.

2. At each workstation, and under each user logon name, load the data base program.

3. If application programs are available for the data base program, run each of those application programs in turn. If an application program is not available, create a simple data base for testing purposes, preferably in a directory created to store data base files.

4. Because data bases are more fixed to a particular directory than document or worksheet files, you need to only check whether records can be added to the data base and written to disk in the default data base directories. Check that only users granted write access can update records, and that users with read/only access cannot update records.

5. If running an application program, select the print option to print the sample data entered to the default network printer. If creating a sample data base outside of an application, use the appropriate command line syntax to reroute the output to the default printer.

6. If more than one printer is attached to the file server, use the CAPTURE command to change the default network printer, or reroute printer output to one of the alternate printers. Print the sample data on each of the alternate network printers.

7. Repeat Steps 1 through 6 for each workstation and user with access to the network.

If any problems are diagnosed, use the guidelines outlined above and the data base or program application documentation to correct the problem and attempt to access the file or resource again. Repeat these procedures until all file, printer, or other resource accesses work as expected.

16. MACINTOSH

APPLETALK

OVERVIEW

AppleTalk is a communications protocol used to connect computers and to share printers and/or other devices on the network. AppleTalk was initially developed to support printing from Macintosh computers to an Apple LaserWriter printer. The original design of AppleTalk was based on a "work" group of six or seven Macintosh computers sharing a LaserWriter. The daisy chain topology mentioned in the LocalTalk section of this document handled this work group.

Once Macintosh computers increased in popularity, advanced topologies for networking connectivity were needed. Apple originally recommended 32 nodes per LocalTalk LAN. When the Active Star topology was used and bridges joined networks together for a larger Internet, the AppleTalk protocol limit was 254 nodes. The 32 node per LocalTalk LAN and the maximum of 254 nodes were conditions of AppleTalk Phase 1. Apple Computer recently released AppleTalk Phase 2. Under Phase 2, the maximum number of nodes per AppleTalk LAN is over 16 million.

Issues associated with installing AppleTalk on Macintosh computers are highlighted in this section. Aspects associated with combining MS-DOS machines with Macintosh hardware in a TOPS environment are discussed in the TOPS section of this document.

INSTALLATION

The AppleTalk protocol software is integrated into the Macintosh Operating System software. The Installer, located on the Macintosh System upgrade disks, updates the Macintosh Operating System software. When the Macintosh Operating System is upgraded on a specific Macintosh computer, it is also necessary to install new printer driver software. Thus, the LaserPrep, LaserWriter, and/or the AppleTalk ImageWriter icons associated with the system upgrade need to be dragged to the Macintosh System Folder.

In an AppleTalk environment, it is helpful if each of the Macintosh computers on the network has the same operating system

software. One of the more common issues on an AppleTalk network concerns printing from one Macintosh computer with a different version of LaserPrep and LaserWriter software than the other Macintosh computers. The LaserPrinter must reset itself to handle these different software versions. Fortunately, these incompatible versions do not shut down the LaserWriter or the AppleTalk network.

OPERATION

The Chooser desk accessory is used to connect or disconnect from an AppleTalk network. Selected from the Apple menu, the AppleTalk network protocol is operational when the "Active" radio button is darkened. To test the LocalTalk and AppleTalk installation, print from a Macintosh to a network printer. An AppleTalk printer can be either a networked ImageWriter and/or a LaserWriter. Currently, the most frequently network printer in the Macintosh environment is the LaserWriter.

To begin printer testing, click on the desired printer icon which is attached to the AppleTalk network (e.g. the LaserWriter). The name of the printer that is ON the network should appear in the window. Select (click on) the name of the printer which should be highlighted. Close the Chooser by clicking on the close box in the left hand corner of the window. Next, print a test file by selecting the Print Catalog from the File menu while at the Macintosh desktop.

AppleTalk networks can be linked together to form an interconnected series of AppleTalk zones. For large network environments, one daisy chain network can be linked with other LocalTalk networks. The AppleTalk protocol provides the software connection for accessing printers on other AppleTalk zones. The Chooser indicates the AppleTalk zones available from the specific Macintosh workstation.

TROUBLE-SHOOTING

The most common troubleshooting activity on an AppleTalk network is determining if the AppleTalk protocol is active. This can be done by opening the Chooser desk accessory and checking to see if the Active radio button is darkened.

Another common difficulty occurs if the LaserWriter or the AppleTalk ImageWriter icons have not been installed into the

Macintosh System Folder. If these network printer icons are not in the System Folder, they will not appear in the Chooser desk accessory.

In performing a Macintosh Operating System upgrade, it is critical that the LaserWriter and AppleTalk ImageWriter icons be updated also. Apple Computer provides updated printer drivers with each system upgrade. Thus, make sure the versions of the printer icons match the Macintosh Operating System version. To determine the System version currently in use by your Macintosh, highlight the System icon in the System Folder and select "Get Info" from the File menu. The same procedure can be used for the LaserWriter and AppleTalk ImageWriter icons.

LOCALTALK

OVERVIEW

In the Macintosh environment, LocalTalk refers to networking hardware. In the EPA environment, the most frequently used cabling for networking Macintosh computers is Farallon's PhoneNet system. PhoneNet uses unshielded twisted-pair wire like that used for telephone wiring systems.

A PhoneNet system can be created by connecting AppleTalk compatible devices (e.g. Macintosh computers and/or MS-DOS machines with a LocalTalk card installed) with PhoneNet connectors and twisted pair wire. The PhoneNet connector attaches to the AppleTalk port of each device to be installed on the network. Use the printer port on Macintosh computers. Each connector is linked to the next connector with telephone extension cables.

PhoneNet connectors are equipped with RJ-11 modular connectors and 7-foot modular extension cables. The PhoneNet unit with a DIN-8 connector is used with Macintosh Plus, SE, and II computers; the LaserWriter IINT printers; and the ImageWriter II printers with installed AppleTalk boards. The PhoneNet DB9 connectors handle Macintosh 128k, 512k, 512ke computers and MS-DOS machines with LocalTalk cards installed. The Apple LaserWriter and LaserWriter Plus printers also require the DB9 connectors.

The PhoneNet system supports four networking topologies which are described in the installation section below. For long term management of large LocalTalk and AppleTalk network systems, it is recommended that a PhoneNet StarController be installed. The StarContoller has 12 ports with each port supporting 3,000 feet of wiring. Thus, one network controller can handle 36,000 feet of wiring. This is discussed further in the Active Star Topology unit of the Installation section.

INSTALLATION

Connectors can be installed using daisy chain, trunk, Passive Star or Active Star topologies. Each of these topologies is discussed below.

Daisy Chain Topology

A daisy chain network topology works well with small installations where all devices are in the same room. The daisy chain

can be constructed quickly using modular telephone extension cables and RJ-11 mounted terminating resistors supplied with each PhoneNet connector. No more than 20 connectors should be used in a single daisy chain. The chain should not exceed 2,000 feet. The ends of a daisy chain should be terminated with the RJ-11 mounted terminating resistor.

Removing a PhoneNet connector from the middle of a daisy chain splits the network into two separate networks. Trunk or Star topologies are recommended for a more durable networking environment.

Trunk Topology

The trunk topology, sometimes called a backbone topology, consists of a single cable linking RJ-11 modular wall boxes installed at each device location. A PhoneNet connector is attached to each device and then connected to the nearest wall box with telephone modular extension cable. The total length of a trunk using 22-gauge, solid copper, unshielded telephone station cable should not exceed 4,000 feet in total network length. Each foot of extension cable branching off from the trunk is counted as two feet of total network length. Terminating resistors should be installed in the wall boxes at the two ends of the trunk cable.

The type of cable installed determines the distance signals will carry on the network. A 22-gauge copper station cable supports a network length of 4,000 feet; 24-gauge copper station cable can handle 3,000 feet; and 26-gauge copper extension cable can handle 2,000 feet. Using shielded wire reduces the maximum distance by approximately 30%.

Passive Star Topology

The Passive Star topology is designed to take advantage of existing telephone wiring. It allows for easy reconfiguration of the network when office personnel are relocated. Trunks and daisy chains can be linked into the Passive Star topology.

A network wired in a Passive Star topology consists of no more than six branches (or spokes) connected together at one central location (the hub). A branch can be a trunk with daisy chains extending from it. The four longest branches must be terminated by installing a terminating resistor inside the wall box furthest from the center of the Star. Any other branches should be less

than 100 feet in length and left unterminated. The total network length (the sum of the lengths of all branches) cannot exceed 4,000 feet.

The following equivalents are used in calculating the effective total network length: (a) One-foot of terminated wall cable, 22-gauge, equals one-foot of the total length; (b) one-foot of unterminated wall cable, 22-gauge, equals two-feet of the total length; c) one-foot of terminated extension cable, 26-gauge, equals four-feet of the total length. These equivalents are intended to ensure that a Macintosh or similar CPU can communicate with another such device anywhere on the network.

Active Star Topology

The Active Star topology is necessary when the total network length exceeds 4,000 feet and requires the use of a PhoneNet StarController (Farallon PN207). The network controller connects a group of daisy chains, trunks, and/or Passive Star networks. There are 12 ports on the StarController. Each of these ports can support 3,000 feet of wiring conforming to the guideline equivalents mentioned under the Passive Star topology section. Thus, one PhoneNet StarController can connect 12 network branches into one large network system of 36,000 feet of wire. The computers connected through the StarController operate as though they were directly wired together on the same physical network. The four longest branches on a StarController should be terminated with a 120 resistor inside the wall box furthest from the star.

A StarController can be incorporated into an existing Passive Star topology. Multiple StarControllers can be connected in a backbone or hierarchical way to build a very large network (greater than 36,000 feet). The network controller package provides software for troubleshooting and managing large networks. This is discussed in the Operational section.

OPERATION

The first step in establishing an operational PhoneNet system involves attaching each computer and printer to the network. Each computer should first be turned off. Next, connect the PhoneNet connector to the AppleTalk port of the computer. On a Macintosh, this is the printer port. Once the PhoneNet connector is attached, turn the computer on and boot up the

system. The Macintosh Operating System will automatically determine that the PhoneNet connector is attached to the printer port. The process of installing and testing the AppleTalk networking software is discussed in the AppleTalk section of this document.

Installation of a printer on the network is a simple process. First, turn the printer off. Next, connect the PhoneNet connector to the AppleTalk port of the printer. Turn the printer on. To test both LocalTalk and AppleTalk connectivity, print from a Macintosh to a printer on the network. This is discussed in the AppleTalk section of this document.

If your PhoneNet system has the Active Star topology, the network can be managed remotely from the network Administrator's location. Through the StarCommand software, it is possible to attach or detach each port on the network, test a network branch for proper termination, and isolate network jamming problems. A separate management bus communicates with PhoneNet StarControllers and is accessed with the StarCommand network management software. The StarController is a standalone device. The StarCommand software runs on a Macintosh and is used only for reconfiguration, testing, and monitoring of the network. A dedicated Macintosh is not required for the StarCommand software.

TROUBLESHOOTING

Below are a few of the basic aspects of troubleshooting a PhoneNet system:

1. Examine all PhoneNet connectors and any connectors which are attached into the Macintosh printer ports and the AppleTalk ports of all printers and other Appletalk network devices (e.g. MS-DOS machines). Ensure that these connectors are plugged into their proper locations.

2. Examine all terminating resistors and ensure that they are installed properly. No more than four resistors should be installed on a single physical network.

3. Select the Chooser desk accessory under the Apple Menu of the Macintosh. Check to see that AppleTalk is "Active". If the PhoneNet system is still not functioning properly, refer to the PhoneNet User's Guide from Farallon Computing. This user's guide comes with the purchase of PhoneNet connectors.

TOPS

OVERVIEW

TOPS, distributed by Sun Microsystems, is a Local Area Network (LAN) protocol which permits the sharing of files in a Macintosh environment. In the EPA environment, TOPS is available to support Macintosh-based computing activities.

TOPS is a distributed network system. This means that any computer on the network can act as both a server and a client simultaneously. File service tasks are distributed among the computers on the network. For example, a Macintosh on the TOPS network can have a series of published files for access by other computers on the system. This same Macintosh can also mount files which other computers have published via TOPS. This distributed approach differs from the dedicated file server approach used by other networking protocols (e.g. Novell's NetWare).

The TOPS network protocol within the EPA environment uses AppleTalk as a transport layer. AppleTalk operates at 230,000 bits per second. This is estimated as approximately 200 times faster than a 1200 baud modem.

It is possible to establish a TOPS network which combines Macintosh and MS-DOS machines. For MS-DOS machines, this requires the installation of a LocalTalk card (e.g. the TOPS FlashCard), the TOPS networking software, and the TOPS NetPrint software. TOPS networking software permits the sharing of files, while NetPrint allows for printing to an AppleTalk LaserWriter printer. Although it is possible to establish a TOPS Network with Macintosh and MS-DOS computers, the following discussion on TOPS focuses only on networking Macintosh computers in the LocalTalk and AppleTalk environment.

INSTALLATION

Installing TOPS in the Macintosh environment is a simple process. Insert the TOPS master disk into the Macintosh computer and run the TOPS Installer program. This installation program will place the TOPS files (SoftTalk, TOPS, TOPS Key, TOPS DA, TOPS Help, TOP Prep, InterBase, PC Icon, UNIX Icon, and Start TOPS) into the System Folder located on the Macintosh hard disk or the boot disk. The Installer will automatically load the TOPS and TOPS

Spool desk accessories under the Apple menu. It is also possible to install TOPS manually by dragging the TOPS files to the System Folder and using the Font/DA mover to load the TOPS and TOPS Spool desk accessories.

TOPS is accessed by selecting TOPS on the Apple menu. When first signing onto the network, a dialog box appears requesting a name for your workstation. This name can be up to 31 characters long. Click the OK box to continue into the network. If a "Sorry, that name is already in use" dialog box appears, click continue. You will be asked to rename your workstation.

OPERATIONAL

The TOPS desk accessory dialog box is divided into three parts. The left side displays the files located on your computer. In the center are command options (open, copy, mount, publish, and help) buttons. The right side of the screen lists the other computers that are active on the network. If there is only one network, this listing is labelled "File Servers". If you are on a large PhoneNet system with bridges and gateways, the name of the zone your computer is located in appears. A zone is a group of networks that are linked to other networks. To find a server not in your zone, click on the name of your zone at the top of the listing and hold down the mouse button. The next level up is labeled "Zones". Move the mouse to that name and release the mouse button. The listing changes to include all of the zones on the network.

Command buttons perform the following functions:

1. Open: Lists the contents of whatever was selected, such as a server, a volume, or a subdirectory.

2. Copy: Permits the copying of individual files from one computer to another.

3. Mount: Attaches the volumes located on remote computers to your own Macintosh. This button changes to "Unmount" when mounted remote volumes are selected. After this command has been executed and the TOPS desk accessory closed, an icon of the mounted volume will appear on the Macintosh computer desktop.

4. Publish: Allows you to make local volumes on your computer available to others on the network. This button changes to "Unpublish" when published local volumes are selected.

5. Help: Provides a detailed explanation of any feature you select from the desk accessory. Select an item and click the Help button to receive a description of the particular item.

Once volumes have been published, others on the network can access your files.

Once volumes have been mounted, you can access these mounted files from the Macintosh desktop on your computer. More detailed discussion on TOPS features can be found in the software manual. The TOPS Spool desk accessory allows for spooling print documents for network printing. This desk accessory is further discussed in the software manual.

TROUBLE-SHOOTING

TOPS occupies memory resources on your Macintosh. There may be situations where it is desirable to run the Macintosh without the TOPS desk accessory loaded. This can be done by pressing the Option key while the Macintosh is booting. A dialog box will appear asking whether you want to install TOPS. A common LAN troubleshooting item occurs when a user has failed to load TOPS, but desires later to access a file on the network. Rebooting the Macintosh should remedy this problem.

Since TOPS is distributed networking software, shutting down your computer can impact other users on the network. Other Macintosh computers could have files mounted on their desktops which correspond to documents and applications on your hard disk. The following dialog box appears if this is the case "Warning: Hard disk has active users. If you continue, they may lose their work." All of the client machines which were attempting to access your files receive a message on their machines. It helps to work out a cooperative agreement among users on the TOPS LAN to handle these difficulties.

If it is not possible to mount a volume after it has been published in TOPS, AppleTalk may not be active on your computer. Check the Chooser to ensure that AppleTalk is active. (See the AppleTalk section of this manual.) There could also be a problem with

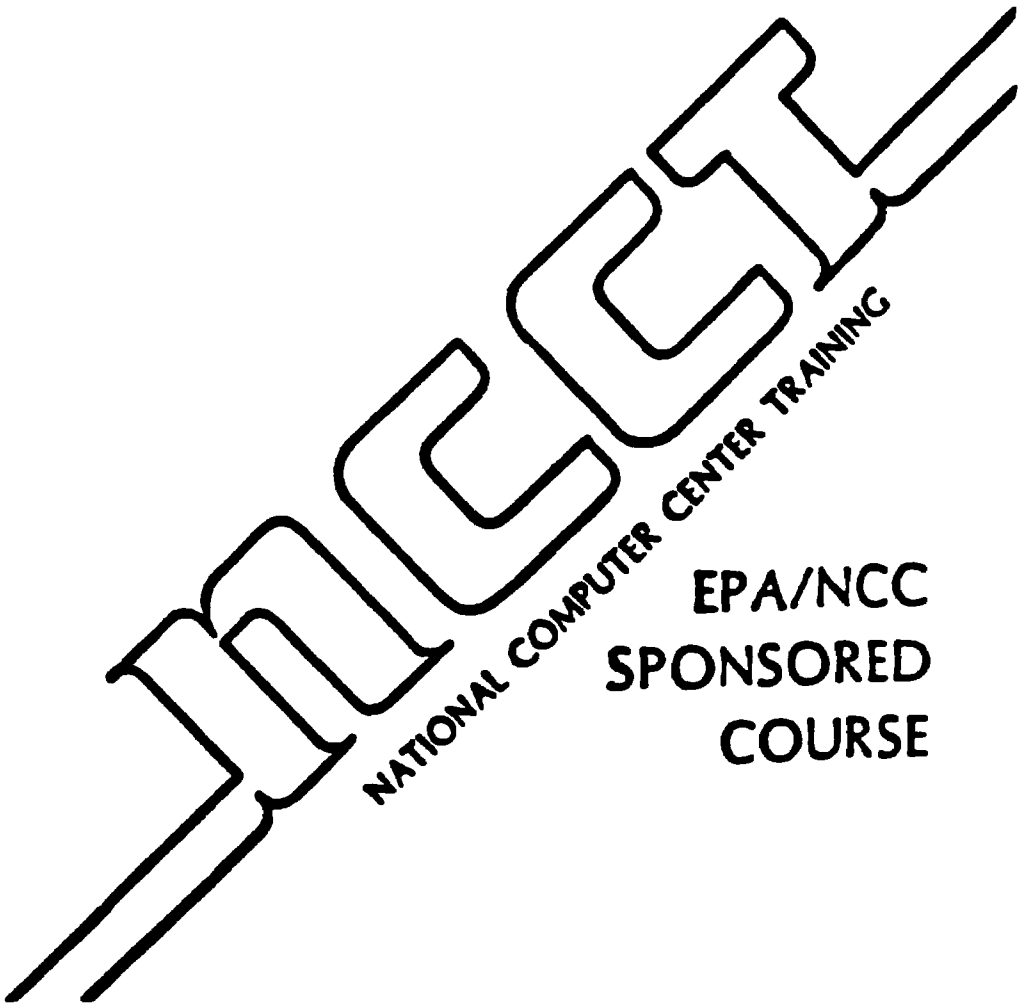
your LocalTalk cable. Check the printer port on your Macintosh to ensure that the PhoneNet connector is installed. (See the LocalTalk section of this manual.)

Appendix A

AGENCY LAN BULLETIN BOARD SYSTEM

210/073

AGENCY LAN BULLETIN BOARD SYSTEM



EPA/NCC
SPONSORED
COURSE

AGENCY LAN BULLETIN BOARD SYSTEM

May 1, 1989

Prepared by LANSYS

EPA NDPD SUPPORT BRANCH
P.O. Box 12314
Research Triangle Park, North Carolina

PREFACE

This manual was prepared by LANSYS as a reference to assist the user in the operation of the Agency's LAN Bulletin Board System.

CONTENTS

1 INTRODUCTION TO BULLETIN BOARD

INTRODUCTION

The EPA Local Area Network (LAN) Bulletin Board System is configured and maintained by the LAN support group, LANSYS, at Research Triangle Park, North Carolina. Its purpose is to provide procedures, problem resolution, documentation, and technical information for EPA LAN Administrators.

SERVICES AVAILABLE

The following services are available as selected from the Main Menu illustrated on Page 1-2.

- TELECONFERENCING allows several users to "converse" with one another over their terminals in an on-line environment.
- OPERATING INFORMATION provides general information on the operation of the Bulletin Board.
- NETWORK BULLETIN is a problem resolution data base. Used for posting questions or a network problem description, network hardware and software information.
- ELECTRONIC MAIL (EMAIL) allows users to leave messages for one another or the system operator (SYSOP).
- FILE LIBRARY is a directory for text and program files with download and upload capabilities. File transfers are made via XMODEM, XMODEM-CRC, or YMODEM.
- USER REGISTRY contains information provided by LAN Administrators pertaining to their particular LAN configurations.

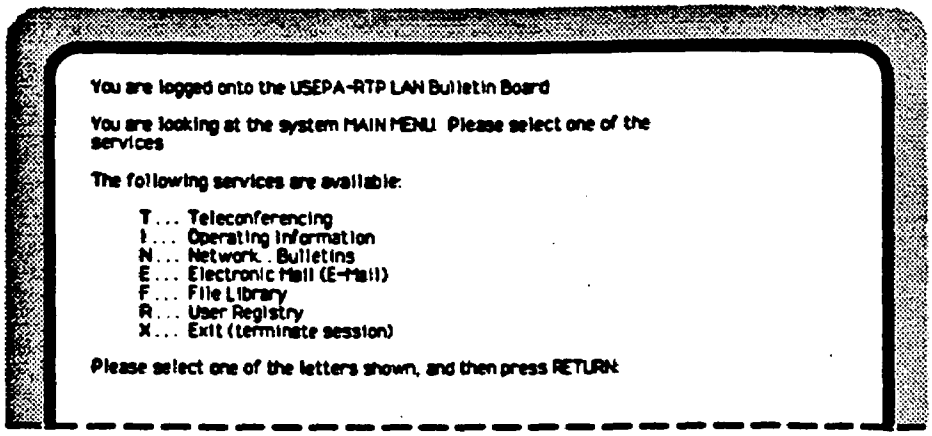


Figure 1. Bulletin Board Main Menu

DEARCHIVING FILES

All files on the Bulletin Board with an .ARC extension have been compressed using a technique called ARCHIVING. These files cannot be used without being dearchived. The program **PKXARC.COM** has been provided for this purpose. Below are some examples for dearchiving files.

PKXARC PKX35A35.ARC	Extracts files from PKX35A35 and places them on the default drive.
PKXARC A:XXXXXX.ARC	Extracts files from XXXXXX.ARC on drive A and places them on the default drive.

The PKX Archiving system files **PKX35A35.ARC** and **PKXARC.COM** are available for downloading from the File Library. **PKX35A35.ARC** contains a read-me file that can be printed for further information on file archiving.

All file transfers via this Bulletin Board are made using the XMODEM, XMODEM-CRC, or YMODEM protocols.

UNIVERSAL USER COMMANDS

These commands are treated in a consistent manner throughout the Bulletin Board:

? <return>	This is your request for HELP. The Bulletin Board replies with details about your options.
X <return>	EXIT. This is your ESCAPE sequence. It returns you to the previous menu.
<ctrl-S>	SUSPEND. This command stops the Bulletin Board from transmitting. It is used when you want to "stop" the screen for a moment. Tapping any key resumes the output.
<return>	ABORT output. When the Bulletin Board is sending long text (i.e., downloading by ASCII method), the output is aborted if you hit the <return> key.

COMMUNICATION SOFTWARE SETUP

Prior to calling the Bulletin Board, you should:

- Ensure that your communications software is capable of handling one of the Bulletin Boards' supported file transfer protocols: XMODEM, XMODEM-CRC, or YMODEM.

- To maintain file transfer integrity, set up your communication parameters as follows:

  DAta = 8 bit
  PArity = None
  STop = 1
  SPeed = 1200, 2400, or 9600
  INfilter = ON (Crosstalk default)

To sign onto the Bulletin Board, you need to access the NCC port selector from your local port selector, or dial into the NCC using one of the following numbers:

For 1200 BPS - FTS: 629-4642 COM: 919-541-4642
For 2400 BPS - FTS: 629-0700 COM: 919-541-0700
For 9600 BPS - Access the NCC port selector via your local port selector.

(If you are not located in a Regional Office or do not have access to the FTS system, you can call

RTP Network Control personnel at 1-800-334-0741 for special access numbers.)

When a connection is established with the NCC, a "Carriage Return" will start the NCC Menu display. (See Figure 2.)

At the Enter Selection prompt, enter: LANBBS. The message *connected* will be returned.

At this point, a carriage return will start the Bulletin Board session.

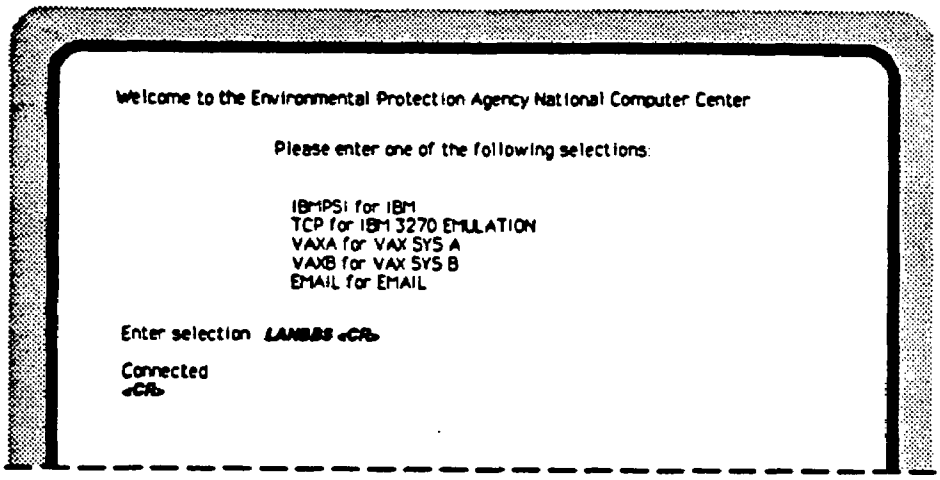


Figure 2. NCC Menu Display

2 NEW USER REGISTRATION

BEGINNING SESSION

When a new user begins a Bulletin Board session for the first time, the following screen appears, requesting user identify and basic information:

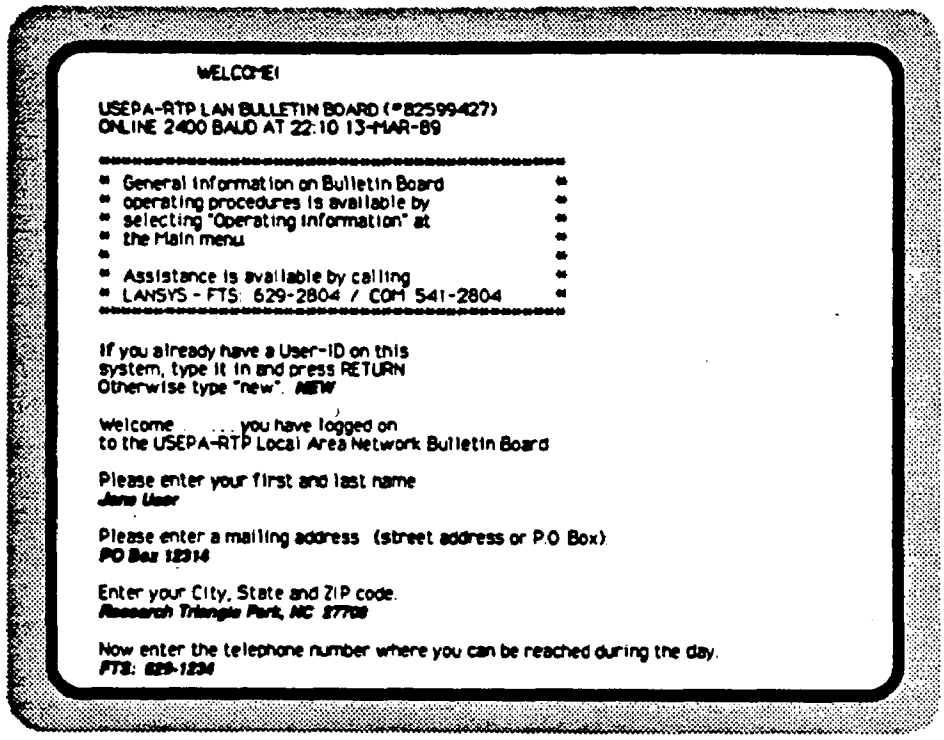


Figure 3. First BBS Screen for New User

The information you provide will be used to identify you as an authorized user. Only properly registered LAN Administrators and authorized users will have full access to all Bulletin Board services. New users will be granted full privileges, usually by the next working day following completion of their user registration.

As indicated by the screen on the following page, the new user is prompted to set up a User-ID and password.

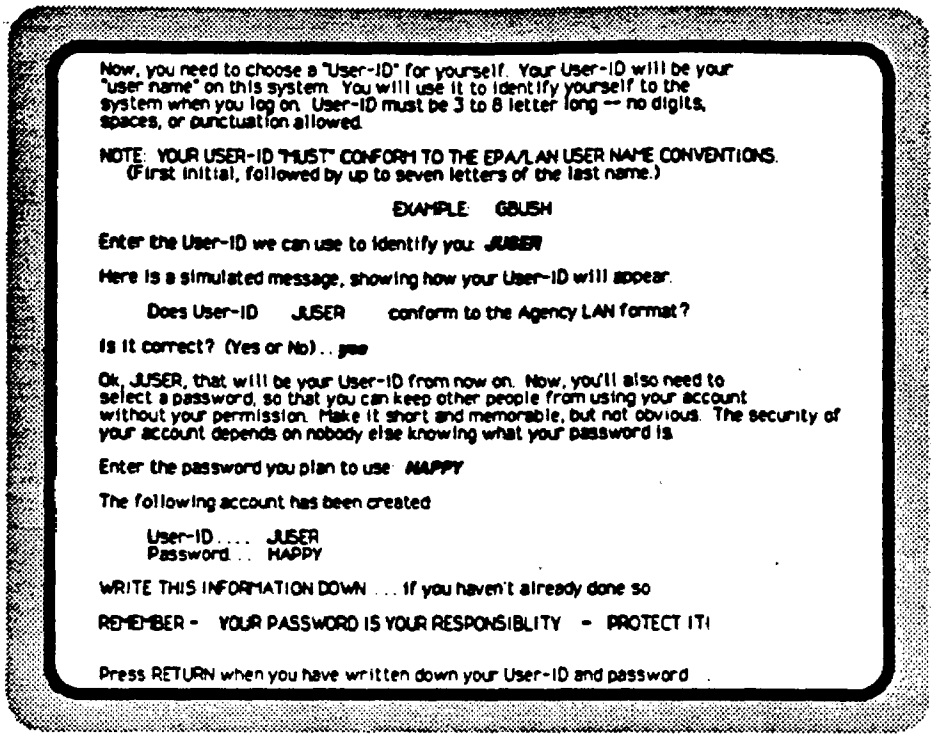


Figure 4. Second BBS Screen for New User

At this point, you are requested to select "R ... User Registry at the Main Menu to complete your user registration.

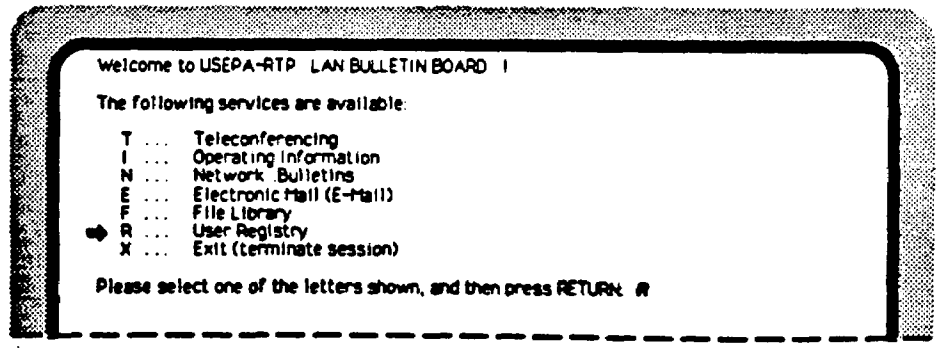


Figure 5. User Registry Option

The information you supplied to the user registration file will be used to confirm your identity as an eligible user of the EPA LAN Bulletin Board System. It may also be used as an aid in analyzing problems, or by other users who may have questions relative to your installation.

DATA ENTRY

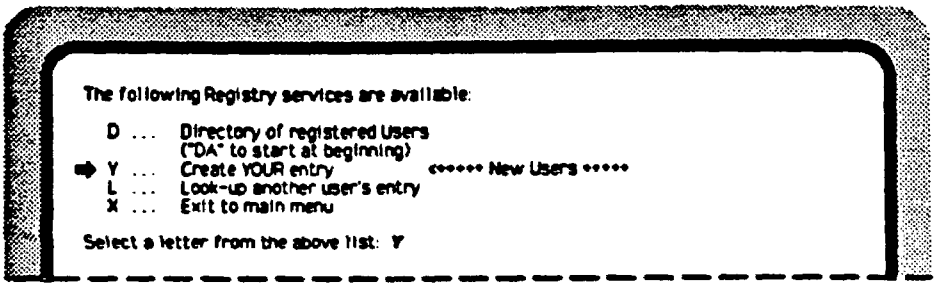


Figure 6. Data Entry Option

You are now prompted to enter data for your entry into the Registry data base. If you prefer not to answer certain questions for personal reasons, type "N/A" for "not available". If you leave the entry questionnaire before completing it, it will not be saved. (You may enter **X** to exit the questionnaire.)

After you have completed your entry, you will be able to edit any part of the data at any time. You should update your information as frequently as required to keep it current.

The following are screens of other services available while in the User Registration Section:

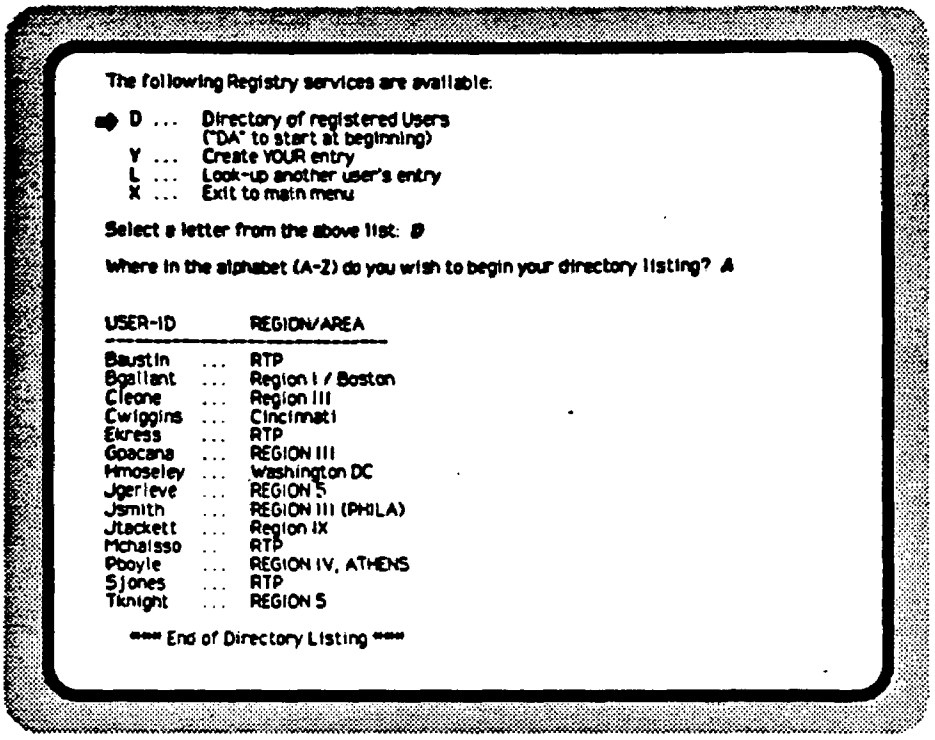


Figure 7. Directory of Registered Users Option

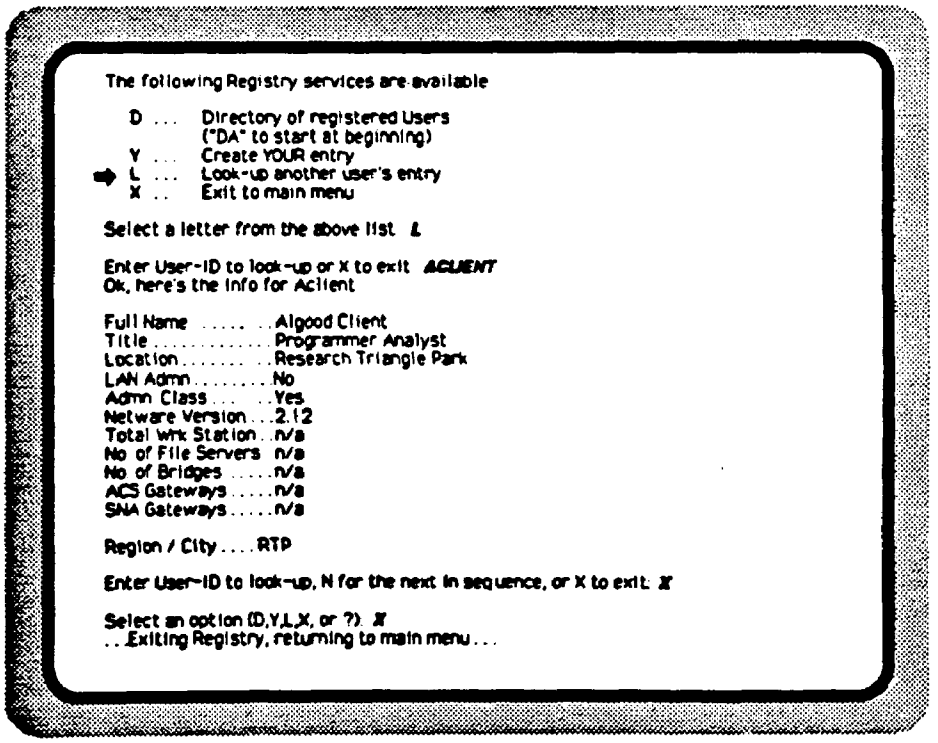


Figure 8. Look-Up Another User's Entry Option

3 TELECONFERENCING

MENU

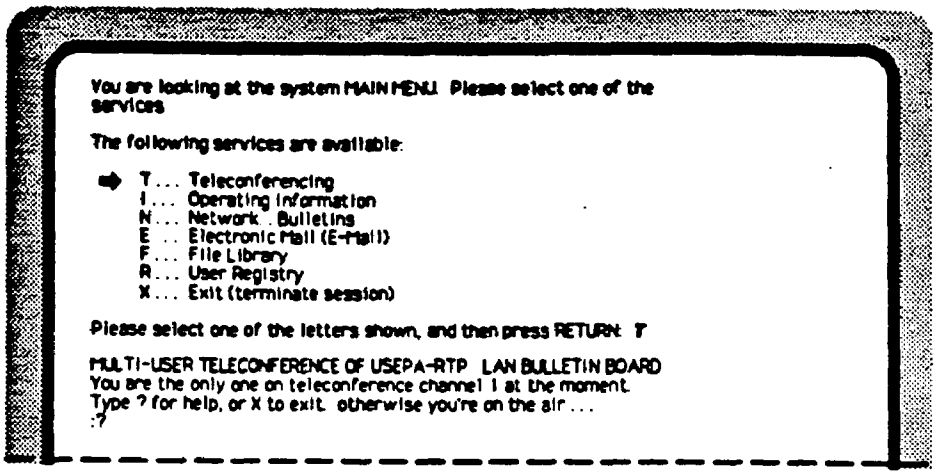


Figure 9. Teleconferencing Option

When you are using teleconferencing, everything you type goes out over the network to everyone who happens to be on your teleconference channel at the time.

SPECIAL COMMANDS

You may use any of the following special commands:

PAGE <Userid>...	Pages you to your teleconference channel.
PAGE ON/OFF/OK	Allows/prevents/encourages others to page you.
WHISPER TO <Userid>...	Sends a private message to another conferee.
/<Userid>...	Shorthand form of the whisper command)
CHANNEL <#>	Switch to channel <#> of teleconferencing.
CHAT <Userid>	Join in a "chat" with a user, or request a chat.
SCAN	Displays all teleconference users on all channels.
UNLIST	Makes your channel number "unlisted" in scans.
LIST	Allows others to see your channel number in scans.

MODERATE <topic>	Sets conference topic and makes you the moderator.
APPOINT <Userid>	(Moderator Only) Resign, make <Userid> moderator.
SQUELCH <Userid>	(Moderator Only) Silence user in your conference.
UNSQUELCH	(Moderator Only) Allows you to talk again.
EXIT or X	Exits teleconference; takes you back to the main menu.

```
:PAGE SYSOP
... Paging Sysop (at main console) ...
:X
Exiting teleconference...
```

4 OPERATING INFORMATION

MENU

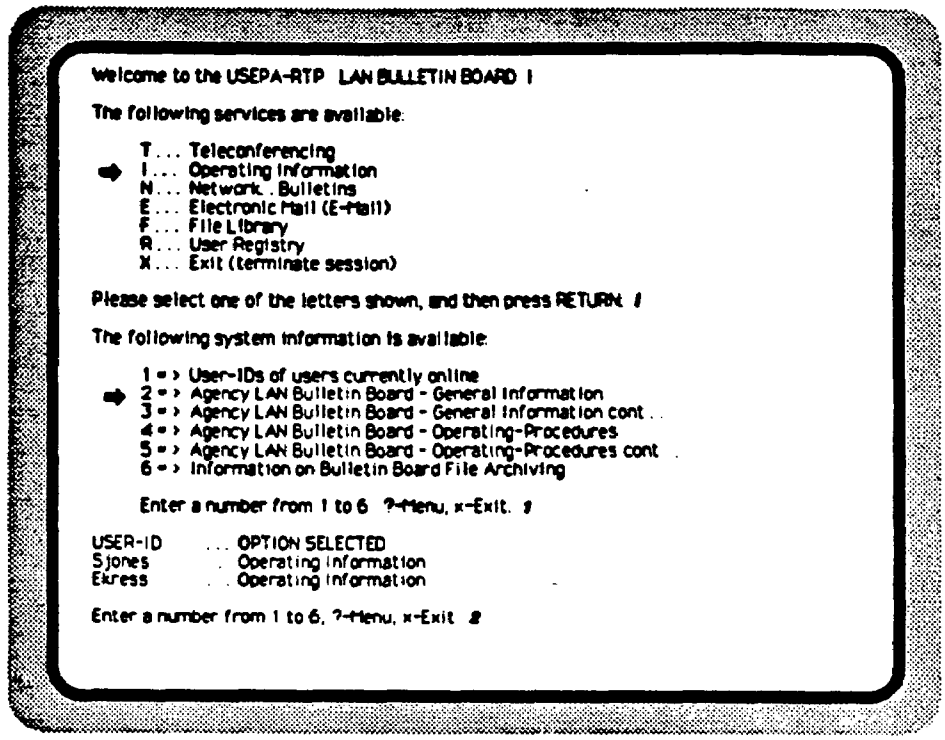


Figure 10. Operating Information Option

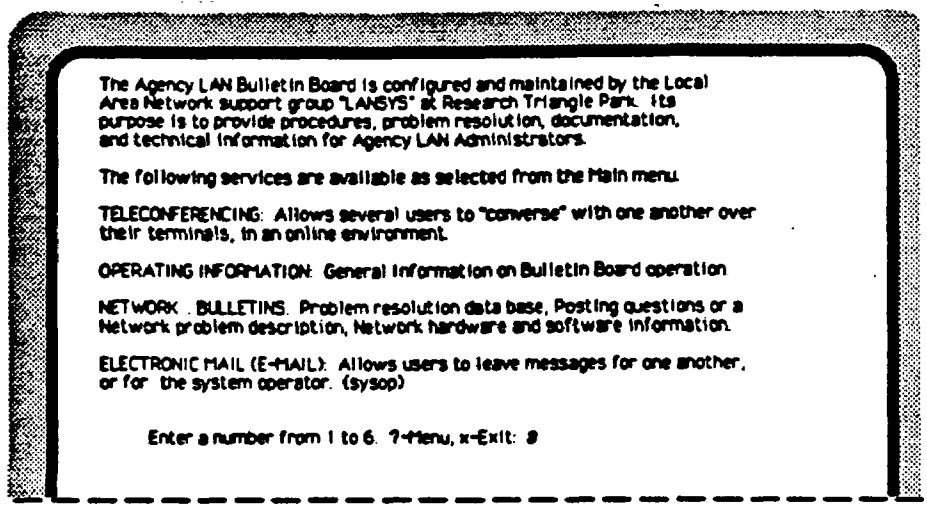


Figure 11. Operating Information Option (Continued)

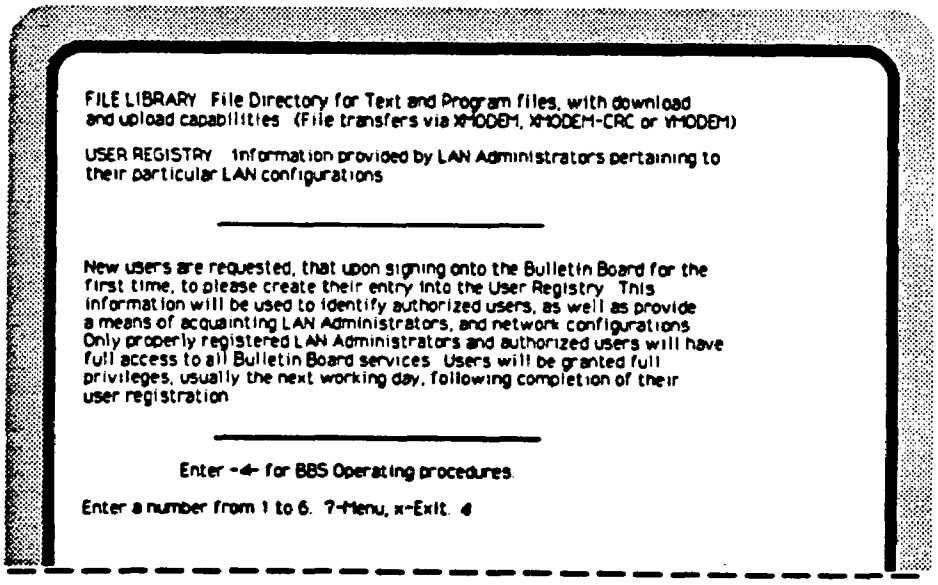


Figure 12. Operating Information Option (Continued)

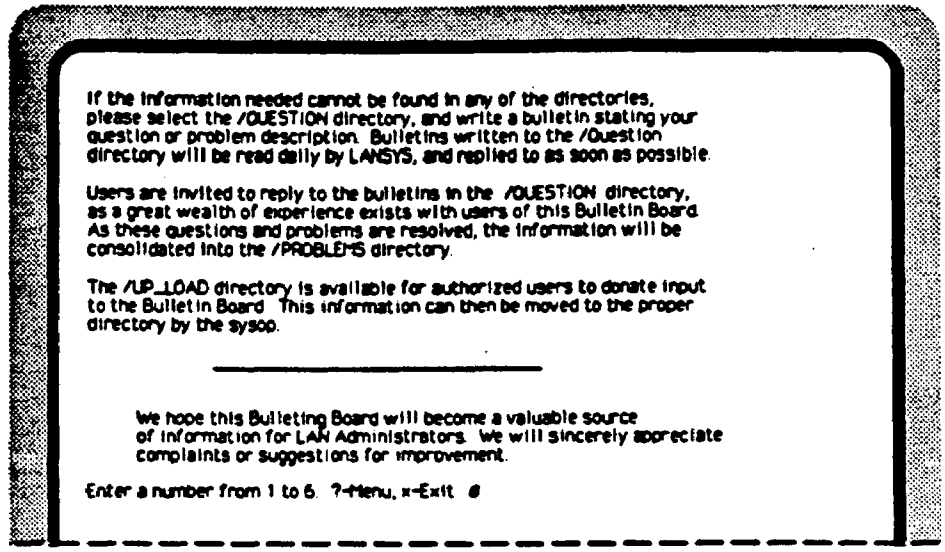


Figure 13. Operating Information Option (Continued)

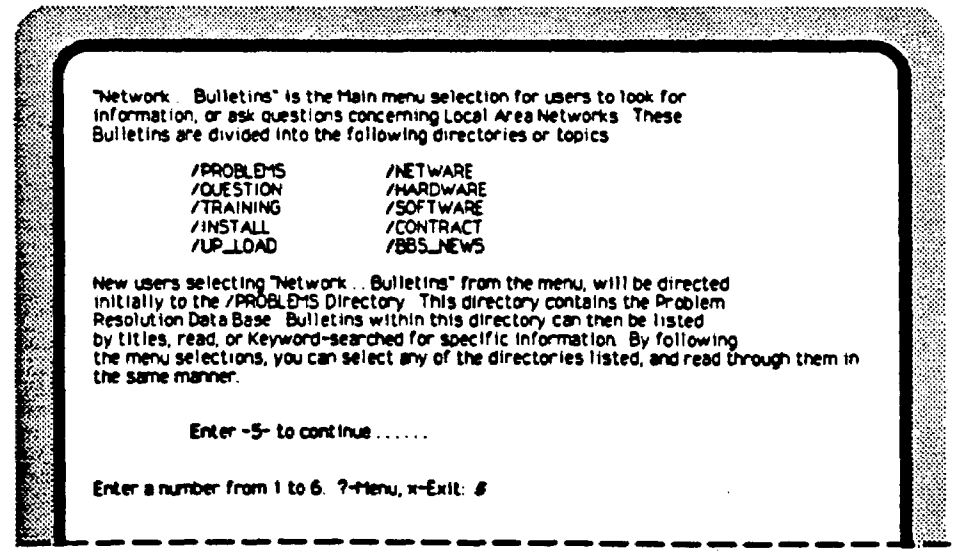


Figure 14. Operating Information Option (Continued)

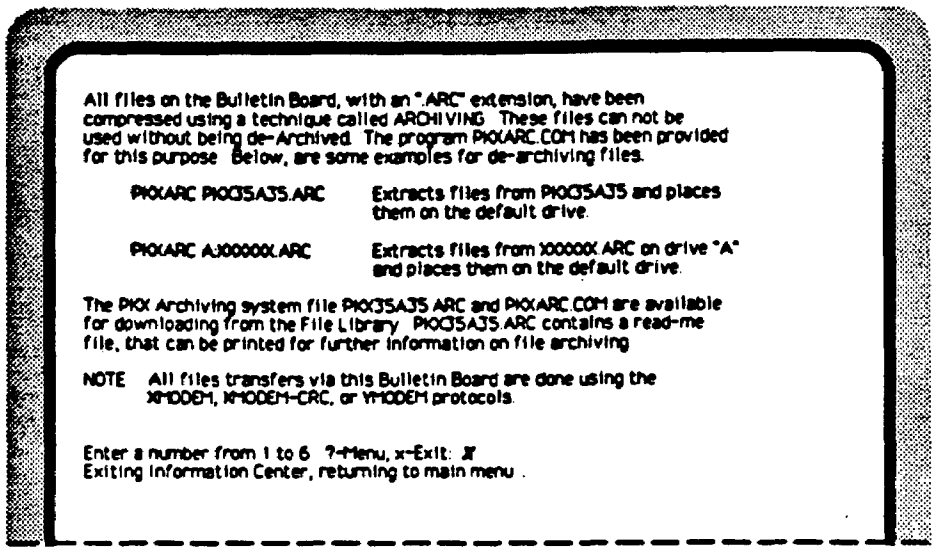


Figure 15. BBS File Archiving Screen

5 NETWORK ... BULLETINS

MAIN MENU

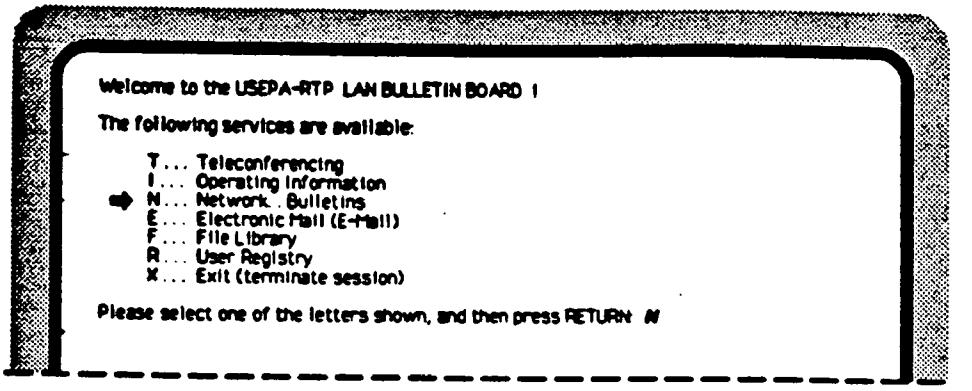


Figure 16. Network ... Bulletins Option

Network ... Bulletins is the Main Menu selection if you require information or have questions concerning the LAN. These bulletins are divided into the following directories or topics:

/PROBLEMS	/NETWARE
/QUESTION	/HARDWARE
/TRAINING	/SOFTWARE
/INSTALL	/CONTRACT
/UP_LOAD	/BBS_NEWS

New users selecting Network ... Bulletins from the menu will be directed initially to the /PROBLEMS directory, which contains the Problem Resolution data base. Bulletins within this directory can then be listed by title; read, or keyword-searched for specific information. By following the menu selections, you can select any of the directories listed and read through them.

If the information you need cannot be found in any of the directories, select the /QUESTION directory and write a bulletin stating your question or describing your problem. Bulletins written to the /QUESTION directory will be read daily by LANSYS and acted upon as soon as possible.

Users are invited to reply to the bulletins in the /QUESTION directory as a wealth of experience exists among users of this Bulletin Board. As these questions and problems are resolved, the information will be consolidated into the /PROBLEMS directory.

The /UP_LOAD directory is available as a means for authorized users to donate input to the Bulletin Board. This information can then be moved to the proper directory by the SYSOP.

AVAILABLE OPTIONS

The following screens illustrate options available under the Network...Bulletins menu:

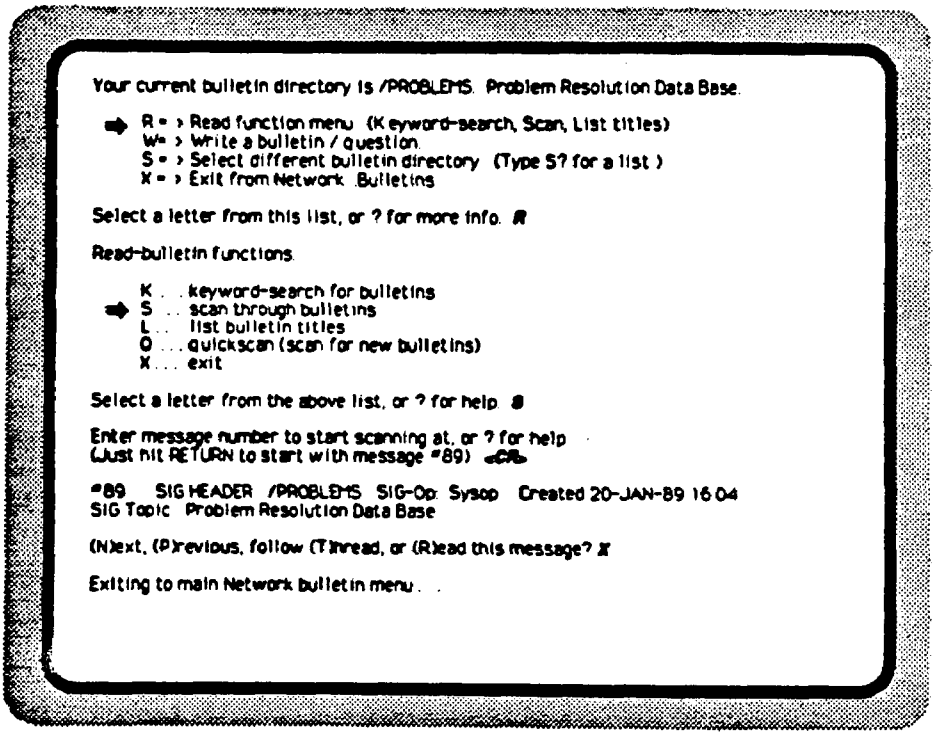


Figure 17. Read Option

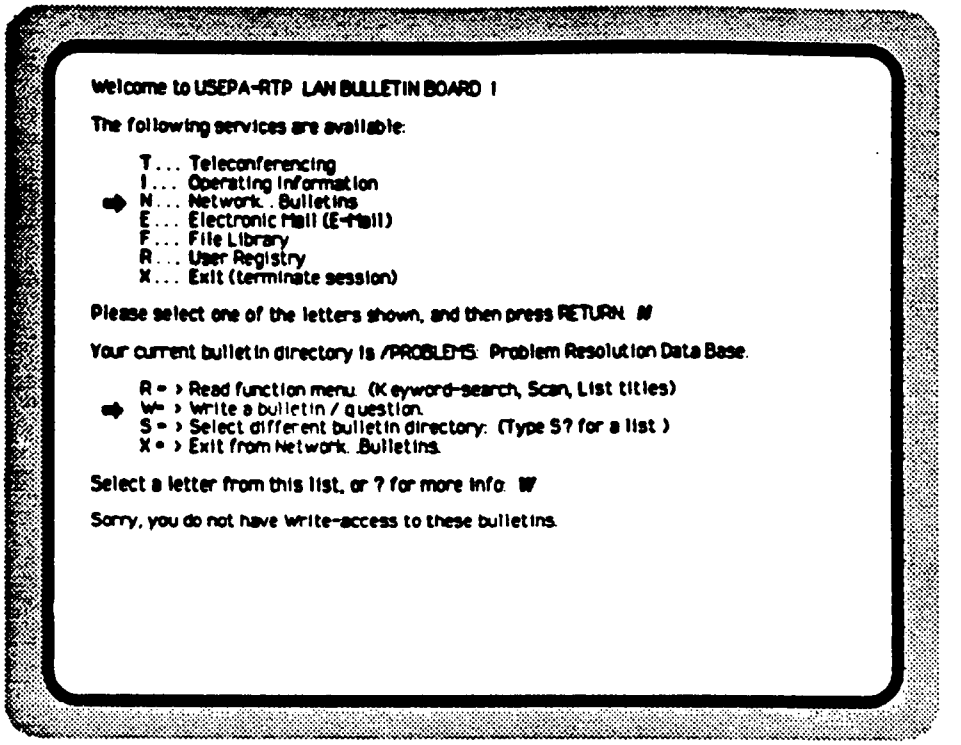


Figure 18. Write Option

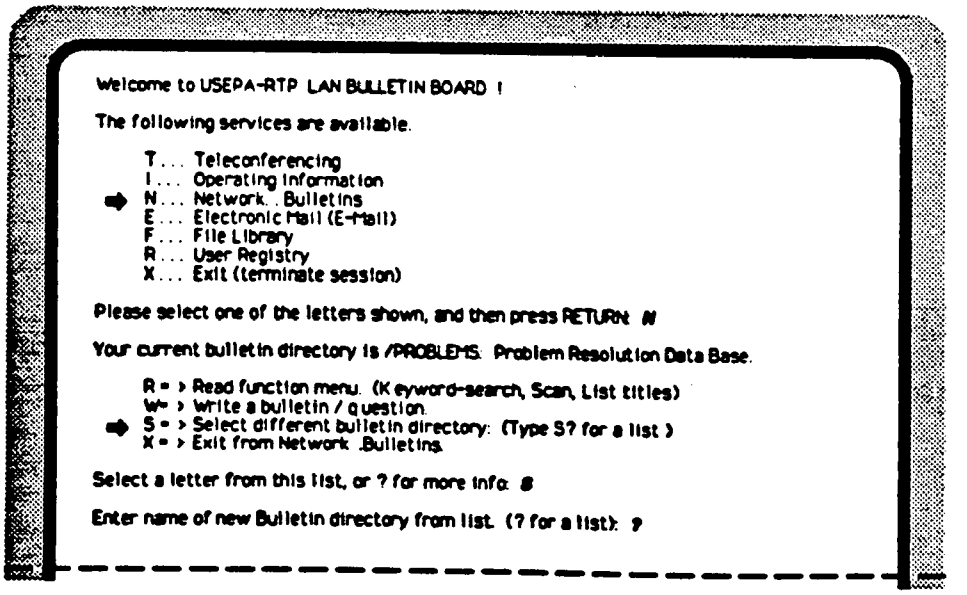


Figure 19. Select Directory Option

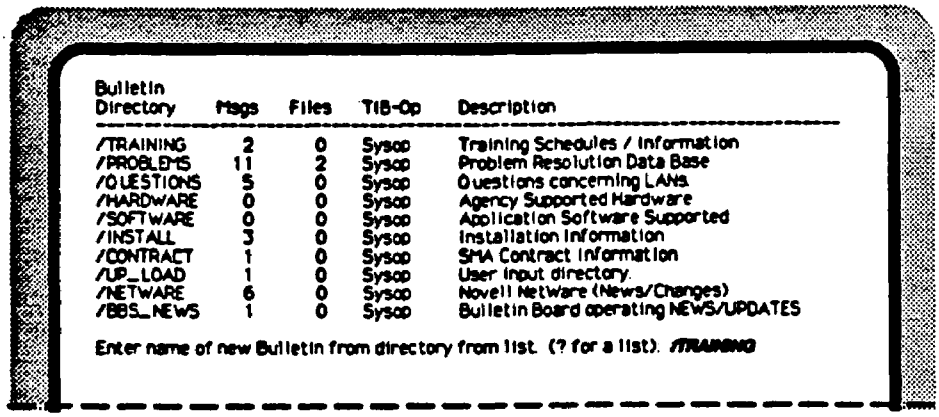


Figure 20. Available Directories

KEYWORD SEARCH Bulletins can be read, or preferably searched using "keywords". While in the Network...Bulletins" menu, enter R at the prompt to begin:

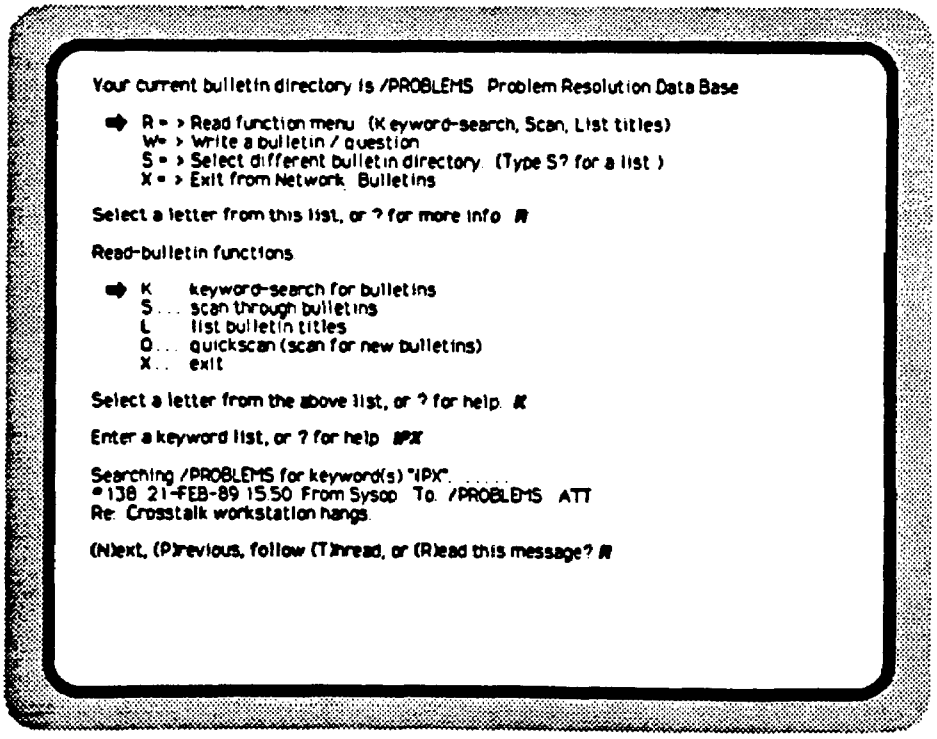


Figure 21. Keyword-Search Option

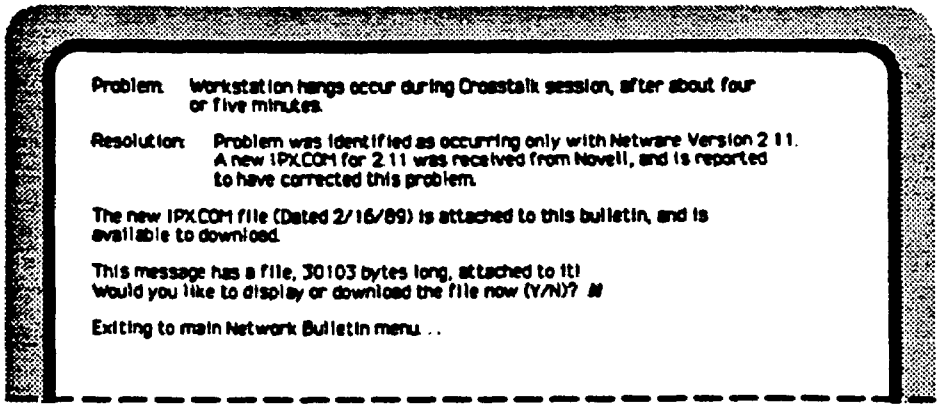


Figure 22. Problem/Resolution Screen

QUICKSCAN

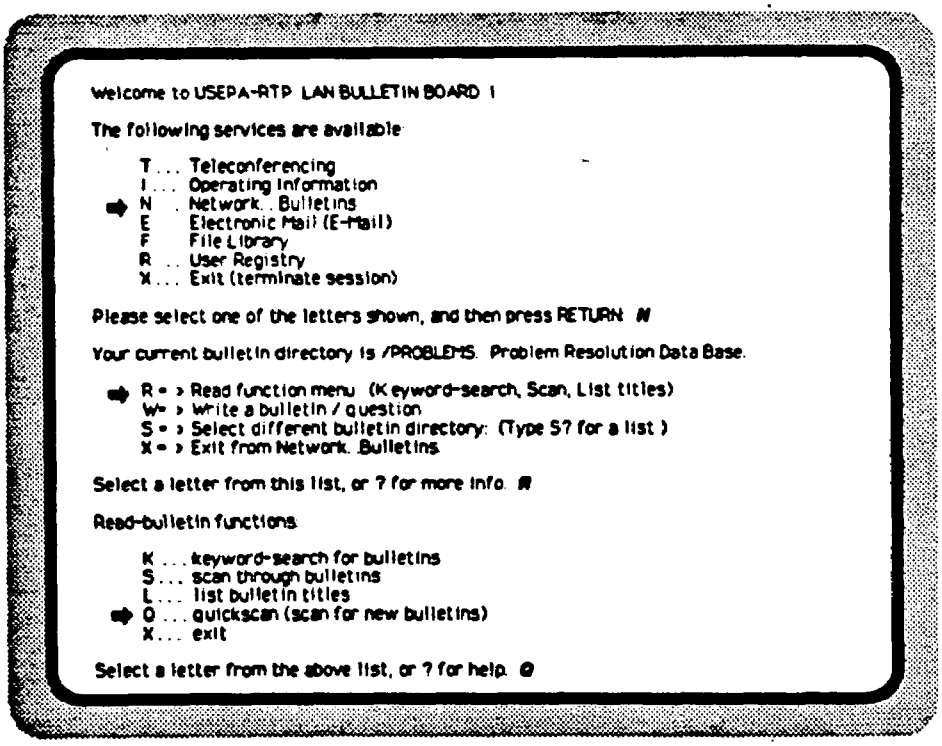


Figure 23. Quickscan Option

Quickscan allows you to scan through all messages in all directories in one operation, stopping only on new messages, or on ones that you haven't read yet.

The first time you choose the "Q....quickscan" selection, you will be prompted through a setup procedure. Be sure to include all the directories into your quickscan at this time. Your list should include:

/Problems	/Training	/Hardware	/Software
/Netware	/Question	/BBS_News	/Contract
/Up_load	/Install		

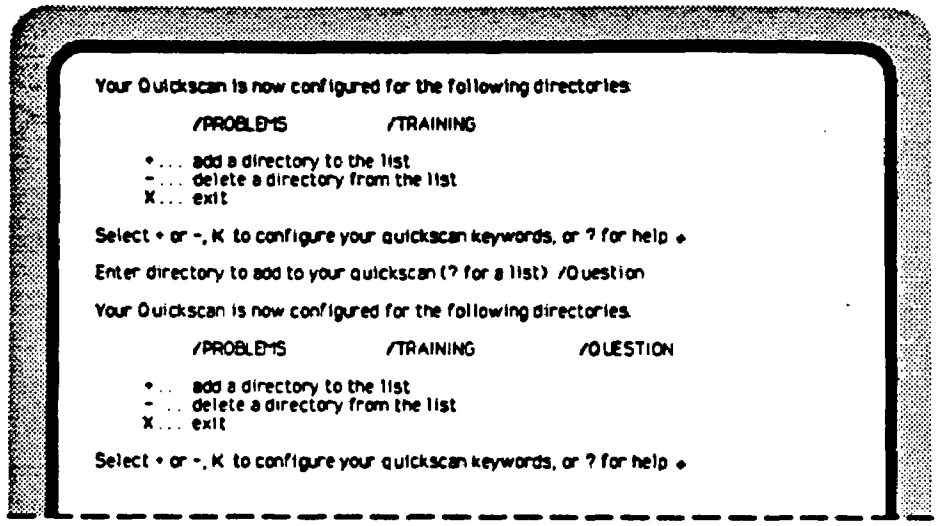


Figure 24. Quickscan Configuration Directory

Once Quickscan is configured, it will search through all the directories, stopping only on new entries (or any that you haven't read yet).

Since this is your first use of the quickscan feature, you have been automatically routed into the configuration utility. By "configuring" your quickscan, you are telling the system what topics to search when you later do a quickscan keyword search, scan, or list.

The system will track the highest numbered messages you have read in each bulletin so that your keyword searches, scans, and listings will only apply to messages that you haven't read before.

The Bulletin topics already present in your quickscan list are there because you selected them (via the "S" option from the main menu) at one time or another. This works for up to 20 topics.

6 ELECTRONIC MAIL (EMAIL)

This feature of the EPA LAN BBS is NOT intended to replace the Agency-standard Electronic Mail System.

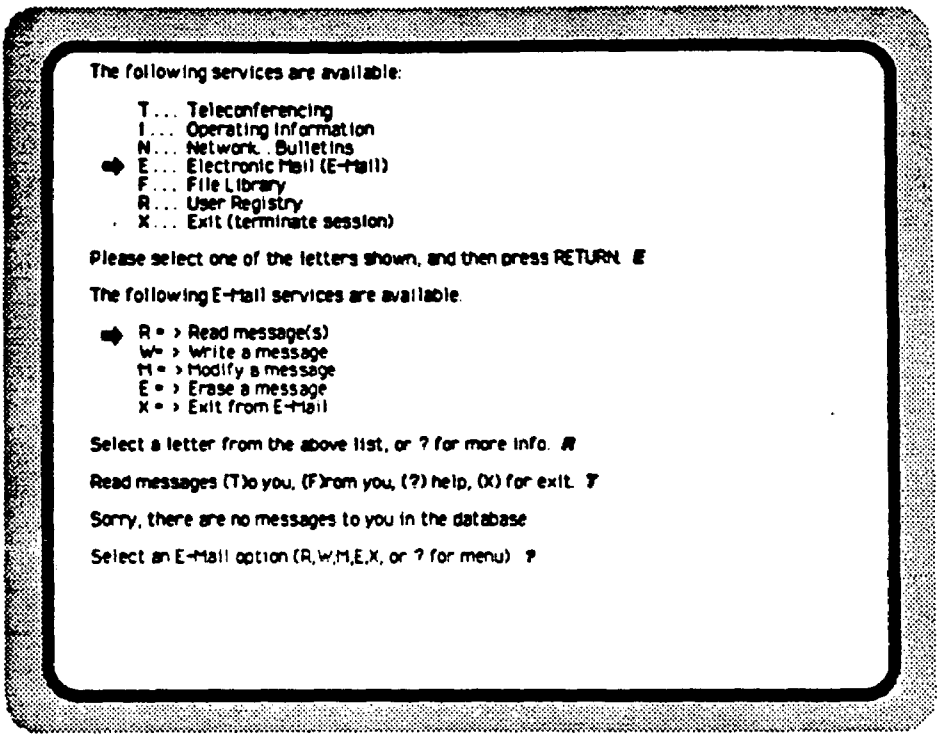


Figure 25. Email Option

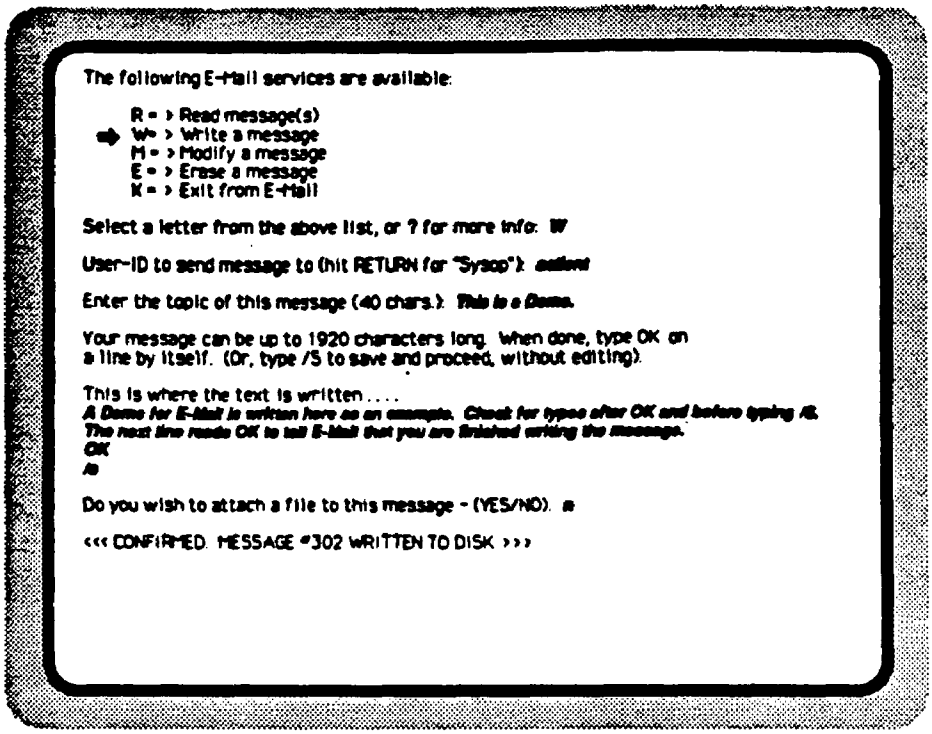


Figure 26. Email Write Option

7 FILE LIBRARY

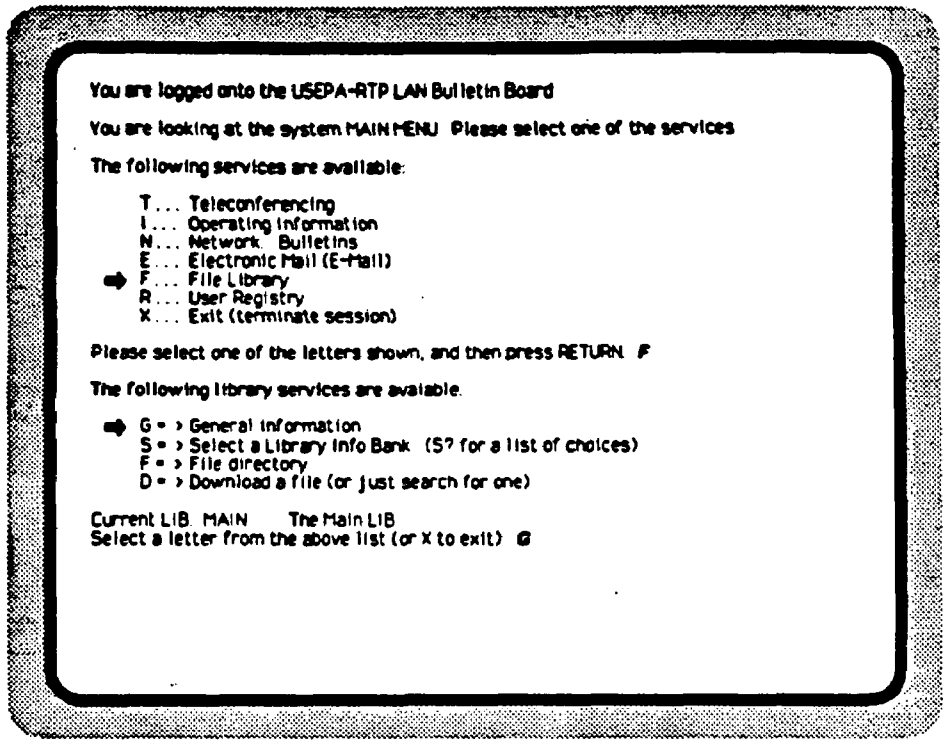


Figure 27. File Library Option

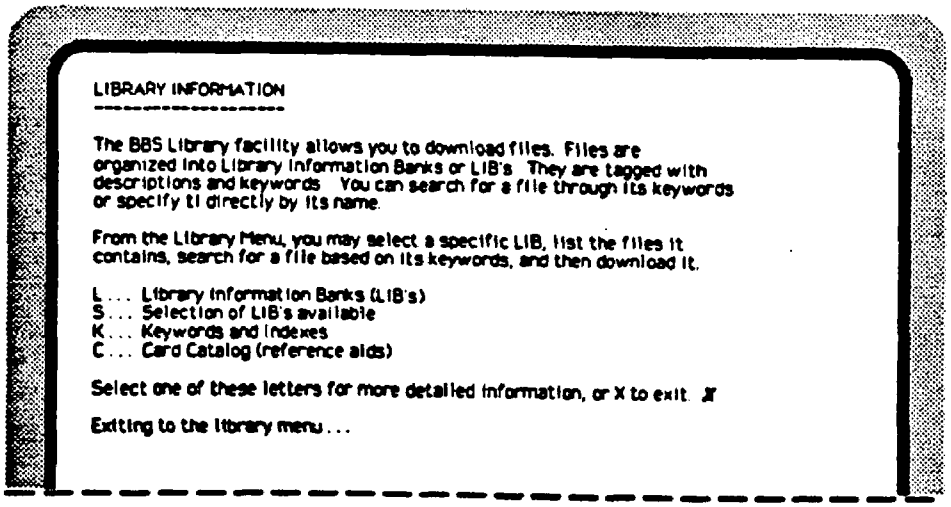


Figure 28. General Information Screen

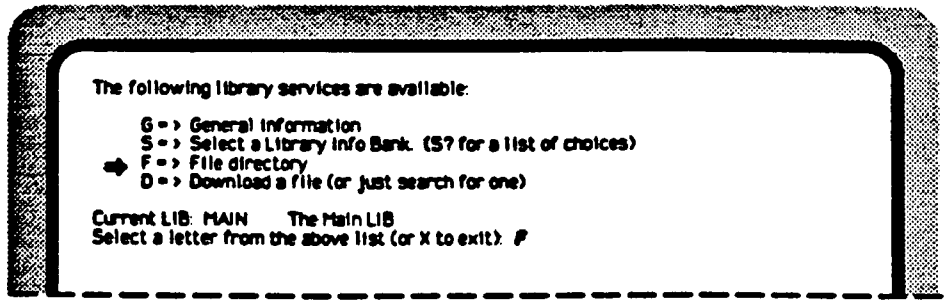


Figure 29. Available Library Services

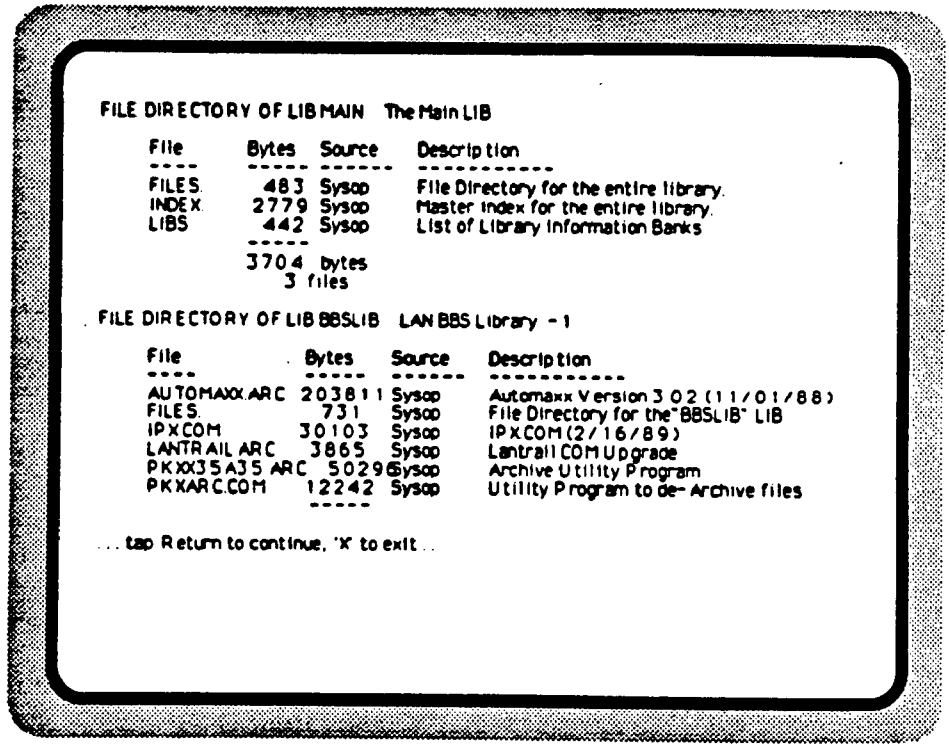


Figure 30. Library File Directory

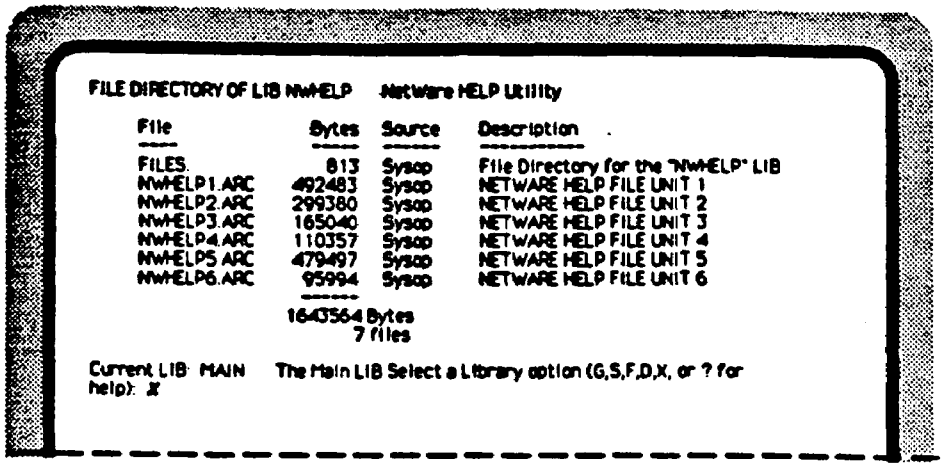


Figure 31. Directory of Help Files

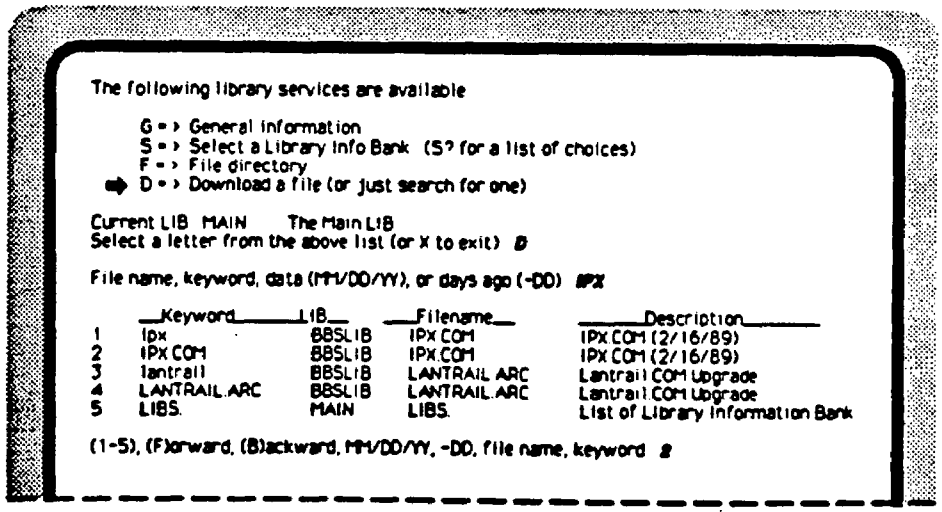


Figure 32. Download File Option

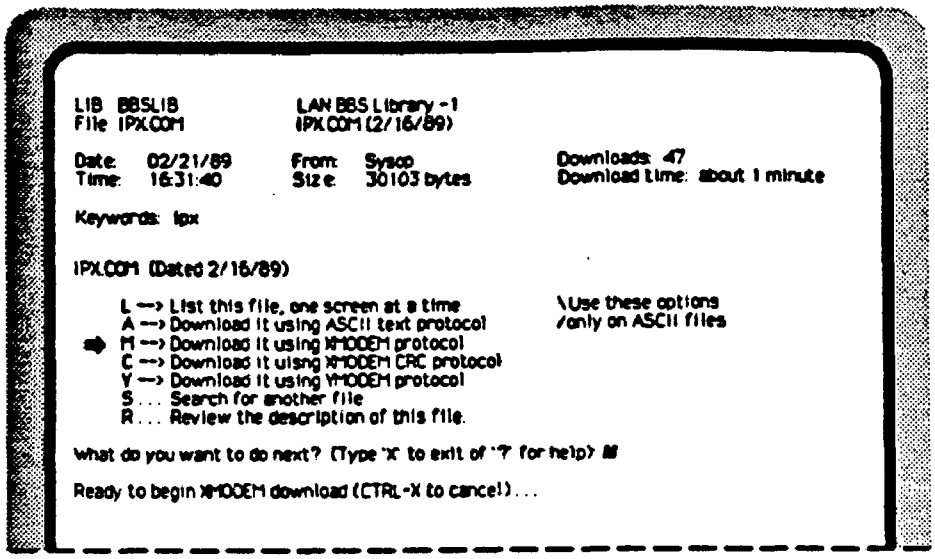


Figure 33. Download XMODEM Protocol Option

Appendix B

DIRECTORY OF BULLETINS

THROUGH DECEMBER 1, 1989

Appendix B

DIRECTORY OF BULLETINS

/PROBLEMS

#89 SIG HEADER: /PROBLEMS SIG-Op: Sysop Created 20-JAN-89
SIG Topic: Problem Resolution Data Base

#124 10-FEB-89 10:41 From: Sysop To: /PROBLEMS
Re: Compaq Portable III

#131 14-FEB-89 15:50 From: Sysop To: /PROBLEMS
Re: Workstation Hangs during LOGIN

#177 01-MAR-89 00:04 From: Sysop To: /PROBLEMS
Re: EPSON speed restriction

#206 08-MAR-89 18:35 From: Sysop To: /PROBLEMS
Re: New IBM PS/2 Mod-30 / 286

#210 08-MAR-89 21:04 From: Sysop To: /PROBLEMS
Re: Token-Ring Adapter Card Interrupts

#241 19-MAR-89 22:50 From: Sysop To: /PROBLEMS
Re: IBM PS/2 MOD-25 "Hangs"

#244 19-MAR-89 23:36 From: Sysop To: /PROBLEMS ATT
Re: INTEL AboveBoard Memory conflicts

#245 19-MAR-89 23:47 From: Sysop To: /PROBLEMS
Re: TELEX Workstation needs DOS 3.2 or 3.3

#293 23-MAR-89 16:09 From: Sysop To: /PROBLEMS ATT
Re: Lantrail Program Errors

#311 28-MAR-89 11:34 From: Sysop To: /PROBLEMS ATT
Re: Workstation Hangs / Crosstalk

#317 29-MAR-89 12:42 From: Jkeefer To: /PROBLEMS
Re: Telex 1280 (Fw by Sysop)

#644 11-MAY-89 13:52 From: Sysop To: /PROBLEMS ATT
Re: Novell Gateway PCOX/GW3270 PTF-169

#645 11-MAY-89 14:58 From: Sysop To: /PROBLEMS ATT
Re: PCOX Communications PTF 176

#647 11-MAY-89 15:11 From: Sysop To: /PROBLEMS ATT
Re: PCOX Communications - PTF 167

#672 19-MAY-89 14:44 From: Sysop To: /PROBLEMS
Re: Epson Equity III+ as ACS Gateway.

#675 19-MAY-89 16:05 From: Sysop To: /PROBLEMS
Re: Epson Upgrade Information.

#890 27-JUL-89 10:21 From: Sysop To: /PROBLEMS ATT
Re: Warning: DBASE IV LAN Compatibility

#1056 06-SEP-89 09:09 From: Sysop To: /PROBLEMS
Re: WordPerfect Office/ACS Gateway conflict.

#1069 11-SEP-89 11:18 From: Npatel To: /PROBLEMS
Re: NETWARE 2.15 AND LANSPOOL (Fw by Sysop)

#1219 12-OCT-89 10:32 From: Gkreizma To: /PROBLEMS
Re: Epson MDA Conflicts with SNA. (Fw by Sysop)

#1250 24-OCT-89 09:41 From: Sysop To: /PROBLEMS ATT
Re: Changing File Servers *ALERT*

End of list!

/HARDWARE

#105 SIG HEADER: /HARDWARE SIG-Op: Sysop Created 24-JAN-89
SIG Topic: Agency Supported Hardware

#1041 29-AUG-89 08:37 From: Sysop To: /HARDWARE
Re: New Style Adapter/A Board.

#1057 06-SEP-89 10:39 From: Sysop To: /HARDWARE
Re: UPS SYSTEM ON GSA SCHEDULE.

#1404 09-NOV-89 15:24 From: Sysop To: /HARDWARE ATT
Re: Renaissance VGA Video Adapter

#1419 29-NOV-89 09:46 From: Sysop To: /HARDWARE ATT
Re: TAPE BACKUP DEVICES - EVALUATION

#1426 30-NOV-89 11:22 From: Sysop To: /HARDWARE
Re: PS/2 MOD - 30/286 as Tape Backup unit

End of list!

/SOFTWARE

#106 SIG HEADER: /SOFTWARE SIG-Op: Sysop Created 24-JAN-89 15:39
SIG Topic: Application Software Supported.

#328 04-APR-89 09:26 From: Sysop To: /SOFTWARE ATT
Re: Arbiter - Operation/Installation

#330 04-APR-89 10:59 From: Sysop To: /SOFTWARE ATT
Re: ACS Gateway Operation/Installation

#405 10-APR-89 16:58 From: Sysop To: /SOFTWARE
Re: Print Management products / LANSPOOL

#761 10-JUL-89 15:45 From: Sysop To: /SOFTWARE ATT
Re: Lotus 123 News

#1075 12-SEP-89 14:31 From: Sysop To: /SOFTWARE ATT
Re: SYTOS Multi Volume Backups.

#1083 19-SEP-89 08:54 From: Sysop To: /SOFTWARE ATT
Re: Statement of LAN-Based Software.

#1414 27-NOV-89 16:33 From: Sysop To: /SOFTWARE ATT
Re: NOVELL NACS GATEWAY - EVALUATION

#1415 27-NOV-89 16:40 From: Sysop To: /SOFTWARE ATT
Re: LAN SYSTEMS - LANSpace - EVALUATION

#1425 30-NOV-89 11:18 From: Sysop To: /SOFTWARE
Re: PS/2 Mod. 30/286 - REQUIRES SYTOS 3.0

End of list!

/INSTALL

#108 SIG HEADER: /INSTALL SIG-Op: Sysop Created 24-JAN-89
SIG Topic: Installation Information.

#129 10-FEB-89 13:37 From: Sysop To: /INSTALL
Re: TIC Gateway Software Dist.

#193 07-MAR-89 22:35 From: Sysop To: /INSTALL
Re: SNA Gateway: Modifying Config.SYS file.

#195 07-MAR-89 23:38 From: Sysop To: /INSTALL
Re: SNA Gateway SHELL.CFG options.

#326 04-APR-89 09:15 From: Sysop To: /INSTALL ATT
Re: ACS Gateway Installation/Operation

#327 04-APR-89 09:20 From: Sysop To: /INSTALL ATT
Re: Arbiter Installation / Operation

#530 26-APR-89 08:34 From: Sysop To: /INSTALL ATT
Re: PCOX and ASCOMIV Documentation

#649 11-MAY-89 15:20 From: Sysop To: /INSTALL
Re: UPS System Installation

#695 06-JUN-89 09:27 From: Sysop To: /INSTALL ATT
Re: Installing Network WordPerfect 5.0

#696 06-JUN-89 09:31 From: Sysop To: /INSTALL ATT
Re: File Server Disk Installation

#697 06-JUN-89 10:22 From: Sysop To: /INSTALL ATT
Re: LOTUS 123 Networker Installation

#744 27-JUN-89 14:59 From: Sysop To: /INSTALL ATT
Re: SNA Batch File / Monitor Type

#759 10-JUL-89 15:37 From: Sysop To: /INSTALL ATT
Re: Increasing DOS environment.

#1043 30-AUG-89 17:50 From: Sysop To: /INSTALL ATT
Re: Revised AUTOMAXX Menu System (8/29/89)

#1413 27-NOV-89 16:26 From: Sysop To: /INSTALL ATT
Re: CORE 380MD HARD DRIVE - INSTALLATION

End of list!

/CONTRACT

#109 SIG HEADER: /CONTRACT SIG-Op: Sysop Created 24-JAN-89
SIG Topic: SMA Contract Information

#917 04-AUG-89 09:07 From: Sysop To: /CONTRACT ATT
Re: IBM PS/2 Model 30 286 Contract Mod.

#1076 12-SEP-89 14:40 From: Sysop To: /CONTRACT ATT
Re: SMA Contract Mods Update 9/11/89

#1078 12-SEP-89 14:52 From: Sysop To: /CONTRACT ATT
Re: SMA Contract CLIN/PRICE Update

End of list!

/NETWARE

#120 SIG HEADER: /NETWARE SIG-Op: Sysop Created 26-JAN-89
SIG Topic: Novell Netware (News/Changes).

#648 11-MAY-89 15:16 From: Sysop To: /NETWARE ATT
Re: Novell Press Release / NetWare 386

#1044 31-AUG-89 08:44 From: Sysop To: /NETWARE ATT
Re: Whats new in NetWare 2.15

#1187 29-SEP-89 14:58 From: Sysop To: /NETWARE ATT
Re: Netware FCONSOLE problem w/ver 100b

End of list!

/BBS_NEWS

#283 SIG HEADER: /BBS_NEWS SIG-Op: Sysop Created 20-MAR-89
SIG Topic: Bulletin Board Operating News/Updates

#284 20-MAR-89 22:06 From: Sysop To: /BBS_NEWS
Re: Bulletin Board 9600 Baud service

#287 21-MAR-89 09:07 From: Sysop To: /BBS_NEWS
Re: Bulletin Board "Quickscan" feature

#373 04-APR-89 14:07 From: Sysop To: /BBS_NEWS ATT
Re: Bulletin Board Operators Guide.

#1035 23-AUG-89 17:05 From: Sysop To: /BBS_NEWS ATT
Re: LAN - Mines (Fw by Sysop, Fw by Sysop)

End of list!

/TRAINING

#88 SIG HEADER: /TRAINING SIG-Op: Sysop Created 20-JAN-89
SIG Topic: Training Information / Schedules

#173 28-FEB-89 21:34 From: Sysop To: /TRAINING
Re: NCC Training Schedule

#412 11-APR-89 16:10 From: Sysop To: /TRAINING ATT
Re: NCC - LAN Training Plan.

#770 12-JUL-89 17:01 From: Sysop To: /TRAINING
Re: Train the Trainer Program

End of list!

/QUESTION

#104 SIG HEADER: /QUESTION SIG-Op: Sysop Created 24-JAN-89
SIG Topic: Questions concerning LAN's

#189 07-MAR-89 16:30 From: Cwiggins To: /QUESTION (1 reply)
Re: SNA Gateway/graphics

#191 07-MAR-89 16:51 From: Cwiggins To: /QUESTION (2 replies)
Re: LAN Spool

#199 08-MAR-89 12:33 From: Sysop To: /QUESTION
Re: LAN Spool (Reply to #191)

#209 08-MAR-89 20:58 From: Sysop To: /QUESTION (1 reply)
Re: SNA Gateway / Screen Distortions

#234 14-MAR-89 10:37 From: Gpacana To: /QUESTION (2 replies)
Re: PRIME BACKSPACE

#237 15-MAR-89 09:18 From: Sysop To: /QUESTION
Re: PRIME BACKSPACE (Reply to #234)

#238 15-MAR-89 15:49 From: Aboze To: /QUESTION (2 replies)
Re: Is th LanManager

#239 15-MAR-89 16:54 From: Sysop To: /QUESTION
Re: Is th LanManager (Reply to #238)

#291 22-MAR-89 17:40 From: Aboze To: /QUESTION (1 reply)
Re: LANTRAIL INSTALL

#296 24-MAR-89 08:52 From: Sysop To: /QUESTION
Re: LANTRAIL INSTALL (Reply to #291)

#313 28-MAR-89 15:05 From: Cleone To: /QUESTION (1 reply)
Re: 115 Meg Disk Upgrade

#315 29-MAR-89 12:48 From: Sysop To: /QUESTION
Re: 115 Meg Disk Upgrade (Reply to #313)

#393 07-APR-89 08:43 From: Jkeefer To: /QUESTION
Re: SNA Gateway / Screen Distortions (Reply to #209)

#395 07-APR-89 09:59 From: Jkeefer To: /QUESTION
Re: PRIME BACKSPACE (Reply to #234)

#466 13-APR-89 14:43 From: Cleone To: /QUESTION (2 replies)
Re: ASCOMIV problems

#468 13-APR-89 16:26 From: Sysop To: /QUESTION
Re: ASCOMIV problems (Reply to #466)

#471 14-APR-89 09:30 From: Jkeefer To: /QUESTION
Re: ASCOMIV problems (Reply to #466)

#519 24-APR-89 11:02 From: Cleone To: /QUESTION (3 replies)
Re: Additional LAN Printers

#537 28-APR-89 08:21 From: Jkeefer To: /QUESTION
Re: Additional LAN Printers (Reply to #519)

#539 28-APR-89 10:33 From: Jkeefer To: /QUESTION (2 replies)
Re: ARBITER

#540 01-MAY-89 11:36 From: Cwiggins To: /QUESTION (1 reply)
Re: ARBITER (Reply to #539)

#580 02-MAY-89 12:02 From: Cleone To: /QUESTION (3 replies)
Re: LAN Communications Questions

#582 02-MAY-89 14:23 From: Jkeefer To: /QUESTION (1 reply)
Re: ARBITER (Reply to #540, Reply to #539)

#583 02-MAY-89 14:45 From: Jkeefer To: /QUESTION
Re: LAN Communications Questions (Reply to #580)

#589 03-MAY-89 08:59 From: Cwiggins To: /QUESTION (2 replies)
Re: ARBITER (Reply to #582, Reply to #540, R*)

#591 03-MAY-89 10:17 From: Baustin To: /QUESTION (1 reply)
Re: Additional LAN Printers (Reply to #519)

#598 04-MAY-89 08:35 From: Jkeefer To: /QUESTION (1 reply)
Re: ARBITER (Reply to #589, Reply to #582, R*)

#600 04-MAY-89 08:41 From: Jkeefer To: /QUESTION
Re: Additional LAN Printers (Reply to #591, Reply to #519)

#605 04-MAY-89 12:42 From: Aboze To: /QUESTION (1 reply)
Re: LAN Space config

#608 05-MAY-89 08:33 From: Sysop To: /QUESTION
Re: LAN Space config (Reply to #605)

#610 08-MAY-89 10:03 From: Baustin To: /QUESTION
Re: Arbiter configuration (Reply to #539)

#615 08-MAY-89 11:26 From: Baustin To: /QUESTION
Re: LAN Communications Questions (Reply to #580)

#619 08-MAY-89 17:57 From: Baustin To: /QUESTION (1 reply)
Re: ARBITER (Reply to #598, Reply to #589, R*)

#621 09-MAY-89 12:57 From: Jkeefer To: /QUESTION
Re: ARBITER (Reply to #619, Reply to #598, R*)

#622 09-MAY-89 13:00 From: Jkeefer To: /QUESTION
Re: ARBITER (Reply to #589, Reply to #582, R*)

#623 09-MAY-89 13:11 From: Cleone To: /QUESTION (1 reply)
Re: WordPerfect Office and MHS

#624 09-MAY-89 14:10 From: Jkeefer To: /QUESTION (1 reply)
Re: Arbiter

#627 10-MAY-89 08:43 From: Sysop To: /QUESTION (1 reply)
Re: WordPerfect Office and MHS (Reply to #623)

#631 10-MAY-89 10:11 From: Sysop To: /QUESTION (1 reply)
Re: Arbiter (Reply to #624)

#632 10-MAY-89 10:20 From: Jkeefer To: /QUESTION (1 reply)
Re: Arbiter (Reply to #631, Reply to #624)

#638 10-MAY-89 16:33 From: Baustin To: /QUESTION
Re: Arbiter (Reply to #632, Reply to #631, R*)

#651 12-MAY-89 09:44 From: Jkeefer To: /QUESTION (1 reply)
Re: CONFIG.UPS

#652 12-MAY-89 12:20 From: Sysop To: /QUESTION (2 replies)
Re: CONFIG.UPS (Reply to #651)

#661 17-MAY-89 11:14 From: Cleone To: /QUESTION (2 replies)
Re: Using Equity III+ as ACS

#662 18-MAY-89 09:21 From: Jkeefer To: /QUESTION
Re: CONFIG.UPS (Reply to #652, Reply to #651)

#663 18-MAY-89 09:30 From: Jkeefer To: /QUESTION (1 reply)
Re: Using Equity III+ as ACS (Reply to #661)

#665 18-MAY-89 14:33 From: Sysop To: /QUESTION
Re: Using Equity III+ as ACS (Reply to #661)

#678 23-MAY-89 16:24 From: Aboze To: /QUESTION (2 replies)
Re: Lan Lotus

#681 24-MAY-89 16:59 From: Sysop To: /QUESTION
Re: Lan Lotus (Reply to #678)

#699 07-JUN-89 11:17 From: Mgehrdes To: /QUESTION (1 reply)
Re: Version 2.15 Netware for Mac

#700 08-JUN-89 15:13 From: Sysop To: /QUESTION
Re: Version 2.15 Netware for Mac (Reply to #699)

#703 12-JUN-89 14:31 From: Cleone To: /QUESTION (1 reply)
Re: ACS Parity Check Error

#722 19-JUN-89 09:29 From: Cleone To: /QUESTION (1 reply)
Re: LAN High Speed Printer/PCOX

#734 22-JUN-89 15:26 From: Cleone To: /QUESTION (2 replies)
Re: WP Office [F7] Problem

#738 23-JUN-89 09:17 From: Sysop To: /QUESTION
Re: LAN High Speed Printer/PCOX (Reply to #722)

#751 06-JUL-89 15:45 From: Sysop To: /QUESTION
Re: WP Office [F7] Problem (Reply to #734)

#764 11-JUL-89 17:36 From: Aboze To: /QUESTION (2 replies)
Re: Use of Dos 3.3 on Equity III+

#768 12-JUL-89 08:19 From: Cleone To: /QUESTION (1 reply)
Re: Use of Dos 3.3 on Equity III+ (Reply to #764)

#769 12-JUL-89 16:57 From: Sysop To: /QUESTION (1 reply)
Re: Use of Dos 3.3 on Equity III+ (Reply to #764)

#822 14-JUL-89 16:05 From: Jgriffit To: /QUESTION (1 reply)
Re: Region 2 Test Site For Netware V2.15

#823 14-JUL-89 16:25 From: Jgriffit To: /QUESTION (1 reply)
Re: Defective ACS WNIM Boards

#837 19-JUL-89 17:19 From: Vbradow To: /QUESTION (1 reply)
Re: Lan Lotus (Reply to #678)

#843 19-JUL-89 17:37 From: Vbradow To: /QUESTION (4 replies)
Re: When using ASCOMIV, it is

#857 20-JUL-89 15:54 From: Sysop To: /QUESTION
Re: Region 2 Test Site For Netware V2.15 (Reply to #822)

#858 20-JUL-89 15:55 From: Sysop To: /QUESTION
Re: Defective ACS WNIM Boards (Reply to #823)

#859 20-JUL-89 15:57 From: Sysop To: /QUESTION
Re: When using ASCOMIV, it is (Reply to #843)

#873 24-JUL-89 10:08 From: Sstonema To: /QUESTION
Re: HP LaserJet (Reply to #868)

#877 24-JUL-89 15:18 From: Jkeefer To: /QUESTION
Re: When using ASCOMIV, it is (Reply to #843)

#878 24-JUL-89 15:23 From: Jkeefer To: /QUESTION
Re: HP LaserJet (Reply to #868)

#892 31-JUL-89 09:36 From: Cleone To: /QUESTION (2 replies)
Re: 380M Core Disk Upgrades

#903 01-AUG-89 16:49 From: Sysop To: /QUESTION (1 reply)
Re: 380M Core Disk Upgrades (Reply to #892)

#905 01-AUG-89 17:06 From: Cleone To: /QUESTION (1 reply)
Re: 380M Core Disk Upgrades (Reply to #903, Reply to #892)

#912 03-AUG-89 14:14 From: Sysop To: /QUESTION
Re: 380M Core Disk Upgrades (Reply to #905, Reply to #903, R*)

#994 14-AUG-89 15:20 From: Cleone To: /QUESTION (1 reply)
Re: Novell 2.15 and Mac Connectivity

#1015 21-AUG-89 14:03 From: Sysop To: /QUESTION
Re: Novell 2.15 and Mac Connectivity (Reply to #994)

#1016 22-AUG-89 10:09 From: Cleone To: /QUESTION
Re: WP Office [F7] Problem (Reply to #734)

#1059 06-SEP-89 14:21 From: Cleone To: /QUESTION (1 reply)
Re: Reply to WP Office/ACS Conflict

#1062 07-SEP-89 15:38 From: Rdreisch To: /QUESTION (1 reply)
Re: LANSPOOL AND Qume Printers

#1068 11-SEP-89 14:30 From: Sysop To: /QUESTION
Re: LANSPOOL AND Qume Printers (Reply to #1062)

#1198 03-OCT-89 13:21 From: Cleone To: /QUESTION (1 reply)
Re: PCOX/2 Remote Printing

#1202 04-OCT-89 16:16 From: Sysop To: /QUESTION (1 reply)
Re: PCOX/2 Remote Printing (Reply to #1198)

#1212 10-OCT-89 15:03 From: Hmoseley To: /QUESTION (5 replies)
Re: RAM Resident Netware printer utility

#1213 10-OCT-89 16:05 From: Pboyle To: /QUESTION (1 reply)
Re: RAM Resident Netware printer utility (Reply to #1212)

#1215 11-OCT-89 12:33 From: Rdreisch To: /QUESTION
Re: RAM Resident Netware printer utility (Reply to #1212)

#1221 16-OCT-89 08:13 From: Sysop To: /QUESTION
Re: RAM Resident Netware printer utility (Reply to #1212)

#1392 01-NOV-89 17:29 From: Hmoseley To: /QUESTION (2 replies)
Re: Transmitting cursor and PGDN using ATERM

#1395 02-NOV-89 10:11 From: Mchaisso To: /QUESTION
Re: Transmitting cursor and PGDN using ATERM (Reply to #1392)

End of list!

LAN ADMINISTRATOR'S TECHNICAL REFERENCE MANUAL QUESTIONNAIRE

(Please return to LANSYS by January 31, 1990.)

		Yes	No
1.	Is the material in this publication presented in a logical and useful manner?	☐	☐
2.	Are the chapters presented in a clear and easy-to-use format?	☐	☐
3.	How do you use this publication:		
	As an introduction to the subject?	☐	☐
	As a reference manual?	☐	☐
	For advanced knowledge of the subject?	☐	☐
	To learn about operating procedures?	☐	☐
	As an instructor of a class?	☐	☐
	As a student in a class?	☐	☐
4.	On a scale of 1-10 (10 being the highest), rate the usefulness of this publication.	_____	
5.	Do you have any suggestions for improving the manual? If so, what would you like to see?	☐	☐
6.	Did you find any errors in this publication? If so, please specify the error and page number.	☐	☐

_____

_____

_____

_____

If you want a reply, please give your name and mailing address:

_____

_____

_____

Send to: LANSYS
EPA National Computer Center
MD-90
Research Triangle Park, NC 27711

--Fold--

Stamp Here

LANSYS
EPA National Computer Center
MD-90
Research Triangle Park, NC 27711

--Fold--