LAN Intensive Care Utilities Version 1.4 - Enterprise Version

for

IBM LAN Server 3.X/4.X/5.X &

IBM Warp Server

Exporter/Importer/Analyzer/Converter Modules

Available
and Ready ™
for OS/2

Available
and Ready ™
for IBM LAN

TABLE OF CONTENTS

Installation

Knowledge prerequisites prior to use

Before we begin, we assume that you are already an experienced LAN Administrator for IBM LAN Server. Along these lines we expect that you know how to set-up/modify users, groups, aliases, and access permissions for your domain using the existing LAN Server tools such as the Full-Screen Interface (FSI), Command Line Interface (CLI), or GUI interface used in LAN Server 4.0/Warp Server. The tools in this package are designed to streamline your administration tasks by supplementing these existing tools by allowing you to do bulk maintenance on your domain.

Complete operation of the LAN ICU package may require patches to your domain controller and requester(s). The patches are available from IBM as well as from our BBS at no charge. These patches do not change the functionality of LAN Server; they primarily fix bugs that can cause problems within your domains. The patches also fix the interface libraries that LAN ICU needs to do its work.

If you are upgrading an existing copy of LAN ICU

To upgrade your existing copy of LAN Intensive Care Utilities, just unzip this version over the top of your previous version and run the REG program as described later in the installation portion of the manual.

To see the new features of this version, please take a look at chapter 13. This chapter details the new features as they have been introduced into the product.

Prior to installation:

1) You must be running LAN Server 3.0 or later
2) The software can run on any OS/2 workstation running LAN Requester. You can also run from any of the servers.

NOTE: If you are using LAN Requester 3.0 with service pack IP7060, you will need to upgrade the requester to either a later or earlier service pack. An error in the IP7060 service pack will cause you to lose administrative previleges to some servers.

If you are using LAN Server 4.0, you should use the latest service pack. You may encounter random Trap D's errors and lock ups without the IBM Service pack. The service pack will need to be applied to the requesters as well as servers.

3) You will need a bare minimum of about 5 megabytes of free disk space on the machine using the LAN ICU software. The larger and more complex your domain, the more disk space you will need to for the exported data.

4) Running the LAN ICU software requires full administrative privileges.   You will need an administrator account to install and use the software.

5) Before you install the software, you must have purchased the right level of users. We sell 4 different versions:

    1-20 Users
    21-50 Users
    51-Unlimited Users
    Site License

If there is no label indicating the number of users that your version is licensed for, then you have the "Unlimited Users" version. The unlimited version and all of the "per user" versions are licensed for use on a single domain only. Site license versions do not check for duplicate copies on multiple domains, nor do they check the user counts on a domain.

Please contact us for a price quote for an unlimited site license at your location. A site license can be substantially less expensive than purchasing individual copies.

If you attempt to install the software on more than one domain, the duplicates will be automatically disabled (this is also a violation of the copyright agreement).

Installation Steps:

1) Create a subdirectory on your hard disk (we recommend the name \ICU).

2) Copy the files from the diskette to the hard disk of the requester (or server).

3) Unzip the source files by typing the command:

```
UNZIP ICUDEMO.ZIP <ENTER>
```

3) Log on to the domain you wish to use this product on. You must be logged on as an administrator.

4) Run the registration program:

```
REG.EXE <ENTER>
```

If you get a message similar to the following message, you have not purchased a copy with sufficent users. Contact your supplier for the right version in that case.

```
┌────────────────────────────────────────┐
│ ▓ Registration Error                    │
├────────────────────────────────────────┤
│                                         │
│   ⓘ   Your domain already has 34 users. │
│       This copy only allows 20 users.   │
│                                         │
│       You cannot register this version in │
│       this domain!                      │
│                                         │
│       Please contact your distributer or │
│       Lieberman and Associates for the  │
│       appropriate version for your domain. │
│                                         │
│   ┌───────┐                             │
│   │ Enter │                             │
│   └───────┘                             │
└────────────────────────────────────────┘
```
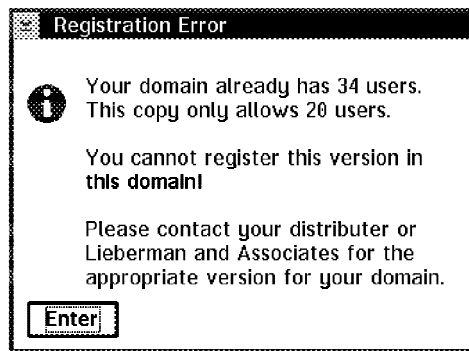
If you have pruchased the **correct version**, you should see the following screen:

```
┌──────────────────────────────────────────────────────┐
│ ▤ LAN Intensive Care Utilities Registration – Ver 1.4 ▩│
├──────────────────────────────────────────────────────┤
│              LAN Intensive Care Utilities            │
│                                                      │
│                     Registration                     │
│                                              ▶       │
│      Domain Name: │DMNPL          │                  │
│     Serial Number: │940812-1-421      │              │
│   Maximum # Users: │50          │                    │
│     Current # Users: │34        │                    │
│                                                      │
│   Customer Name: │Enter User Name        │           │
│   Company Name: │Enter Company Name      │           │
│                                                      │
│  ┌─────────┐  ┌─────────┐      ┌──────┐              │
│  │ Register│  │░░░░░░░░░│      │ Exit │              │
│  └─────────┘  └─────────┘      └──────┘              │
└──────────────────────────────────────────────────────┘
```

To customize your copy of LAN ICU on your domain do the following:

A) Enter your name and company by overtyping the Customer and Company Name Fields:

Customer Name: Philip Lieberman

Company Name: Lieberman and Associates

B) Click on the Register button:

Register

C) If everything went OK, then your should then receive the following confirmation message:

Registration Write

User customization completed <OK>
Thank You!

OK
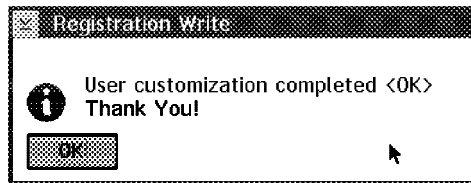
D) Click on the OK button to return to the main registration screen.

E) Click on the Exit button to close the registration program:

Exit

5) Now that you have LAN ICU installed, **please fill out your registration card and return it to us**. We use the supplied information to supply you with announcements of updates and fixes.
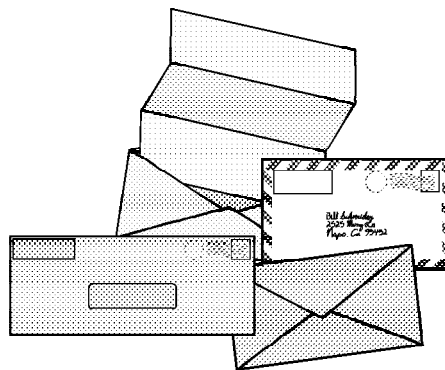
Chapter 1 - Product Introduction

Overview

Thank you for purchasing Lieberman and *Associates LAN Intensive Care Utilities (LAN ICU) for IBM LAN Server.* We are constantly making improvements to this product. You can get the latest version of this product by dialing our BBS at 310-550-5980. If you have any problems or comments about the product, you can reach us at 310-550-8575 or at 800-829-6263 (USA/Canada). If you prefer, you can also reach us via EMAIL on our BBS, Internet, or Compuserve (see the front cover for addresses).

We are constantly making improvements. Our BBS is the fastest way to get these updates. We will also post announcements of these upgrades via Compuserve and IBMLINK. If you do not have access to our BBS, we can also send you the upgrades via mail. When you purchase the product, please indicate what the best update method is on the warranty card you mail back to us.

This product has been tested with both LAN Server 3.0 and 4.0 products and should allow you to perform complete administration in both environments. If you encounter any problems running our product, feel free to contact us for assistance in problem resolution. We are interested in any suggestions you might have in improving the product.

What the product does

This product provides a series of tools to maintain the operation of your LAN Server domain. The export tool (LU.EXE) creates a text file of your entire domain. Within the output of the exporter you will find many valuable reports to assist you in day-to-day operation of your LAN. The output of the LU.EXE program forms the input for batch editor (BA.EXE) tool also known as the importer. The batch editor allows you to create simple ASCII command sections to add, delete, and update users, groups, aliases, public/private applications and more. The last tool is the analyzer (AN.EXE) that identifies and fixes problems within your domain.

You will find separate chapters in this manual that detail the operation of each of the utilities. In the chapters you will also find tips and techniques on using the utility package.

Situations where LAN ICU is used

One of the most helpful thing about LAN ICU is that the exporter will provide you with a comprehensive list of every user, alias, group, and ACL in your domain. It also reports problems that it finds in the domain. This gives you a head start on problems before they get out of control.

If a user reports that they are missing something in their profile, you can simply look them up in the export output file and you will see everything there is to know about the account. If there is a problem with an alias, you can look it up and, again, find everything there is to know about the resource. The export utility also provides a permuted list of all ACLs in the domain. The ACL listings show you permissions assigned to each user and group, as well as permissions sorted by resource name and server.

The exporter also reports on the users of each alias. This is a handy feature to see the relative loads on each resource. It also reports aliases referenced by users, but do not exist on any server in the domain (orphan aliases). This last feature allows you to find and fix the dreaded 'Some of your aliases are not functioning" message.

A fail-safe feature of the exporter is its report of all servers that are currently down in the domain. This is an important feature in cross domain administration. Migration must be performed with all servers up, or improper domain administration might result.

Domain backup and recovery

LAN Server does provide a BACKACC and RESTACC utility, but as you have probably discovered, this does not backup the DCDB, and in some cases you may be creating corrupted backups without knowing it. We felt that an ASCII version of the domain would be a more reliable backup format. The only limitation is that we cannot currently export the passwords of your users.

Automated domain creation

Some LAN Server administrators are responsible for building many identical domains for remote corporate placements. You can use the import and export utilities to build standard images and then incorporate customizations as needed in the ASCII file. The big advantage of this method over manual builds is that you are guaranteed a consistent and tested domain image. LAN ICU is also a lot faster!

Consolidation/separation of resources

Since many domains are not static, the administrator must periodically move users from domain to domain as well as reassign aliases to different machines to even out system loading. Using the export and import utilities (with some editing of the export file), you can move users, groups, aliases, and ACLs from machine to machine. The importer provides both creation and deletion sections for all resources so that effective pruning of the domain can also be accomplished.

Domain problems

We have designed an analyzer program to go through your domain and look for problems and correct them. The analyzer looks for problems created by LAN Server itself, and by improper or incomplete resource creation. The analyze program also checks for inconsistencies in user accounts based on a set of rules that you create. This rule-based analysis assures that security has been consistently applied across all users. The rule base is also used to make sure that all users get the complete set of resources (aliases and applications). The rules are set by creating sections that define what are the defaults for each group membership. Overrides are also provided for exceptions to rules.

The analyze program will explain each problem it encounters and will give you the option of either ignoring the problem, or offering to fix it for you. If the problem cannot be corrected, an explanation of a resolution will be provided (some things cannot be corrected without patches to LAN Server). A log file is created to record all changes made to the domain by the analyze program as well as by the importer.

Licensing

Each copy of LAN ICU is licensed on a **per-domain basis**. The software license of this initial release allows you an unlimited number of users as well as unlimited number of servers on that domain. If you are doing cross domain administration, you must have **a separate copy for each domain**. For example, if you are going to run the tools within this package on two domains, you will need two licensed copies of the software.

If you will be running LAN ICU on multiple domains, site licensing is the least expensive way to purchase this software. Product discounts vary based on the number of copies purchased.

License Agreement

This is a legal and binding contract between you, the end user, and Lieberman and Associates Design and Engineering Group. By using this software you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, you should return the software and documentation as well as all accompanying items promptly for a refund.

1. Your Rights. Lieberman and Associates Design and Engineering Group hereby grant you the right to use a single copy of the LAN Intensive Care Utilities for IBM LAN Server on a single domain. You may not use the exporter, importer, or analyzer on any domain other than the one it was purchased for;unless you have purchased additional copies for each domain.

2. Copyright. The SOFTWARE is owned by Lieberman and Associates Design and Engineering Group and is protected by United States copyright law and international treaty provisions. Therefore, you must treat the software like any other copyrighted material (e.g. a book or musical recording) except that you may either (a) make one copy of the SOFTWARE solely for backup and archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup and archival purposes. The manual is a copyrighted work also--you may not make copies of the manual for any purpose other than the use of the software.

3. Other Restrictions. You may not rent or lease the SOFTWARE. This software is intended to be used on a single domain controller. If you break apart the LAN into multiple domains, you must purchase additional copies of this software if you wish to operate the software on multiple domains. You may not reverse engineer, decompile, or disassemble the SOFTWARE that is provided solely as executable programs (EXE files). If the SOFTWARE is an update, any transfer must include the update and all prior versions.

Limited Warranty

The diskette(s) and manual that make up this software are warranted by Lieberman and Associates to be free of defects in materials and workmanship for a period of 30-days from the date of your purchase. If you notify us within the warranty period of such defects in material and workmanship, we will replace the defective manual or diskette.

The sole remedy for breach of this warranty is limited to replacement of defective materials and/or refund of purchase price and does not include any other kinds of damages.

Apart from the foregoing limited warranty, the software programs are provided "AS-IS", without warranty of any kind, either expressed or implied. The entire risk as to the performance of the programs is with the purchaser. Lieberman and Associates Design and Engineering Group do not warrant that the operation will be uninterrupted or error-free. Lieberman and Associates Design and Engineering Group assume no responsibility or liability of any kind for errors in the programs or documentation of/for consequences of any such errors.

This agreement is governed by the laws of the State of California.

Should you have any questions concerning this Agreement, or if you wish to contact Lieberman and Associates Design and Engineering Group, please write:

Lieberman and Associates Design and Engineering Group
221 N. Robertson Blvd. Suite C
Beverly Hills, CA 90211-1703

Components of LAN ICU

To help introduce this package to you, the following table outlines the different utilities and files that comprise the Lieberman and Associates LAN ICU package.

Export **LU.EXE**	Create output files that contain the complete definitions of your users, groups, aliases, and access control lists (ACLs) for the resources on each server.
Import **BA.EXE**	Allow you to add users, groups, aliases, and ACLs via ASCII files created via the exporter utility. You can also create your own ASCII files with the users, groups, aliases, or ACLs you want to add. To assist you, the importer allows you to specify defaults for each type of resource so that you can minimize your typing (you just type the unique properties of the item(s) to be added).
Analyze **AN.EXE**	This utility goes through your domain looking for inconsistencies in user definitions, alias definitions, groups, and missing or inadequate access permissions for users. It is interactive and does not make any changes to your domain without confirmation. The utility is also designed to remove corrupted entries in the DCDB as well as recreate mangled user accounts..
Convert **CV.EXE**	The LAN Requester program in all version of LAN Server can produce a "Domain Definition Report' that describes the resources in that domain. This utility converts the report into a format that can be used to by the importer program (BA.EXE). This file can be used to build a LAN Server 3.0 or 4.0 domain.
Register **REG.EXE**	When you first receive your copy of LAN ICU, please run this program to setup your personal and company name in the package. This information is printed on all log and operation reports.
Unlock Key **ICUKEY.DAT**	This file contains the unlock key for your copy of LAN ICU. If you are running the demo version, we can send you this file electronically to unlock you copy of LAN ICU.

|	
Patch **LRSD.DLL**	Patch file for your domain controller if it is running LAN Server 3.0 or 3.01 without any service packs applied. You do not need this patch if you have applied IP7045 or later. This file replaces the like named file in \IBMLAN\NETLIB of your domain controller.
Import File **STOOGES.ICU**	Sample import file for batch importer (BA.EXE) file to add users and groups via import file.
Import File **NOSTOOGE.ICU**	Sample import file for batch importer (BA.EXE) file to remove users and groups via import file.
Rules File **RULES.ICU**	Sample rules file for analyzer (AN.EXE) to determine proper user account settings. This file must be modified to handle your particular domain configuration.
Decompress File Utility **UNZIP.EXE**	OS/2 program to decompress ZIP files.
Example of Capture **EXAMPLE.LOG**	Example output from the LU.EXE exporter program
Print Manual **MANUAL.CMD**	Batch file to print out this manual to an HP LaserJet located on LPT1.
Manual **ICUMAN.ZIP**	Zipped version of HP LaserJet print file of this manual. You can print this file by unzipping it. Next use the command: `PRINT /B ICUMAN.HPL`
LATEST	Latest information about LAN ICU that did not make it into the manual. This file contains the latest features that were added to your package.
Read.Me	Information about installing and buying the product.

Chapter 2 - Export Utility Overview (LU.EXE)
Export Utility Overview (LU.EXE)

You can run LAN ICU from any workstation in your company that is running OS/2 2.X/Warp and at LAN Requester 3.0 or later. The utility will redirect its requests to your domain controller for remote execution. You can operate on multiple domains without having to log off the current domain and log on to the new domain. The ability to operate on multiple domains with one logon requires that you have the same userid and password in all domains you will be administering.

You must have administrator privilege on the domain for these utilities to work. It is possible to run many of the utilities at the physical domain controller without this privilege, but we do not recommend this method.

The best way to learn how to use these utilities are to run the exporter (LU.EXE) and examine its output. Because the output of the utility can be very large (5 megabytes for a 1800 user domain), we recommend that you install the utilities on a disk partition that has plenty of room for capture files.

Exporter (LU.EXE) generates complete details of domain

C:>LU

User Details

Group & Members

Alias Definitions

Public Application

Server/ Workstation Details

Access Control Lists

Alias Cross Reference Report

Modal Report/ Security Policy
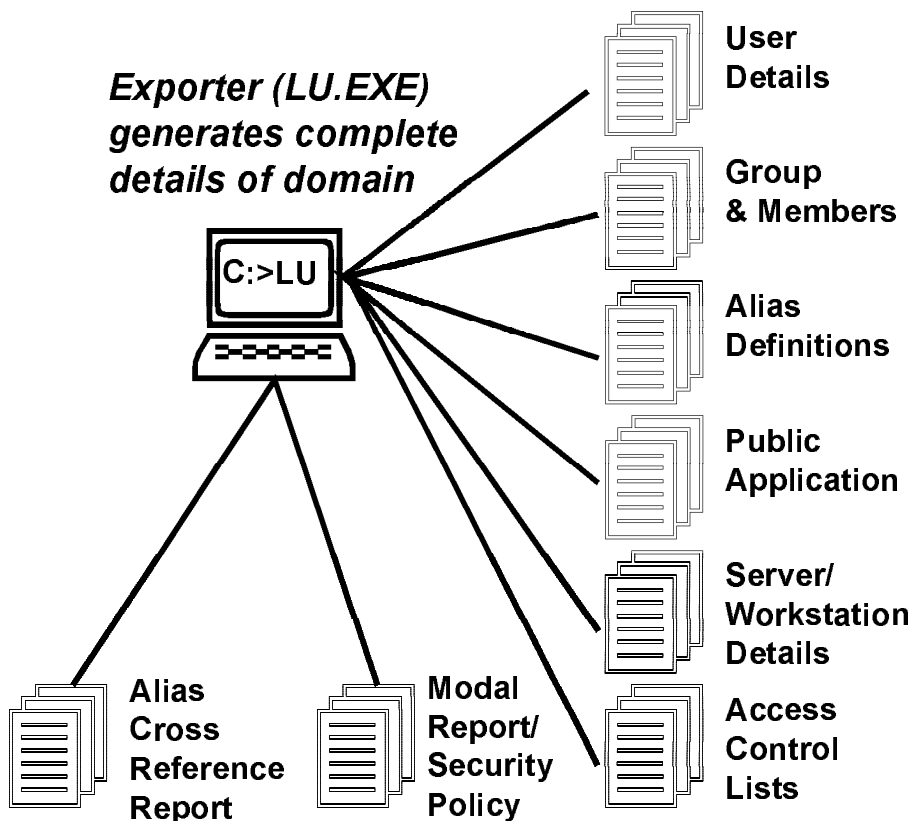
Using the Export Utility (LU.EXE)

To see the command line options of the exporter, try the following command:

LU ? <ENTER>

You should then see the following output (new options may be available):

```
LU.EXE (version 951228) - syntax:  LU [switches] [-O:LOGFILE]
 'LAN Intensive Care Utilities' for IBM LAN Server
  Copyright 1994,1995 - Lieberman and Associates Design
     and Engineering Group

 -[Q]uiet - turns off output to console only
 -[V]erbose flag - provides additional status information
 -[O:]Output_log_file_name (Send report to a file (append))
 -[AO:]Output_log_file_name (Send report to a file (append
mode))
 -[RO:]Output_log_file_name (Send report to a file (replace
mode))
 -[ALI]AS Report
 -[USE]ERS Report
 -[UN:StartUserID],EndUserId (limits actions
     to single/range of userids/groups
   Applies to [USER], [GROUP], and [ACCESS] (ACES)
 -[SER]VERS Report
 -[APP]LICATIONS (Public) Report
 -[XRE]F Cross reference Aliases and Users Report
 -[BAN]NER Report
 -[MOD]ALS Report (System Security Policy)
 -[WOR]KSTATION Settings Report
 -[GRO]UPS Report
 -[ACC]ESS Control Report
 -[BAD] ACLs Report - warnings about bad ACLs (builds
FIXACL.ICU)
 -[RSRC:]Server, Resource (or alias), Recursion(Y/N)
      (ACLs by server & path)
 -[PAS]SWORD - Extract encrypted password plus user data
 -[XPA]SSWORD - Extract encrypted password exclusively
      (no user data)
 -[DOM:DOMAIN_NAME] (override logon domain name)
 -[SRV:SERVER_NAME] (override primary domain controller name)
 -[E{A,D,U}:{[USE]ER,[GRO]UP,[ALI]IAS,[APP]LICATIONS,[ACL],
      [ACE], [ALL]}
  Change Export [List] sections to [Add],[Delete],
      or [Update] sections
 -[ISRV:SERVER_NAME,SERVER_NAME...] Operate only on these
servers
 -[XSRV:SERVER_NAME,SERVER_NAME...] Exclude these servers
 -[F]{[F]ile, [D]irectory, [N]on-existent, [P]rint,
      [C]omm, p[I]pe} ACL filter

Selecting any one report, disables the rest unless they are
 also selected on the command line.  You may put the parameters
 in any order you wish.  Capitalization is not important.
```

The output of the exporter is normally sent to the screen. The default setting for report categories is to provide all reports. Using the command line options you can limit the reports to the ones you are interested in only. The output of the exporter can also be captured into a file of your choice.

For example, to capture the alias definitions only to a file called ALIAS.ICU, enter the following command:

LU -ALIAS -O:ALIAS.ICU <ENTER>

To capture the users and public application definitions to a file called USERS.ICU, enter the following command:

LU -USE -APP -O:USERS.ICU <ENTER>

Capturing the entire domain for the first time

To get a complete capture of your domain, perform the following steps:

1) Log-on to your domain with an administrator account.
2) Enter the following command to capture the domain to an ASCII file.

LU   -O:DOMAIN.ICU <ENTER>

NOTE: If you do not want to see the data go screaming by on the screen, enter the following command (added -Quiet command added) instead:

LU -Q -O:DOMAIN.ICU <ENTER>

Depending on the size of your domain, this could take anywhere from 1 minute to an hour to capture everything in your domain. This command will simultaneously echo data to the screen as well as to a capture file called: DOMAIN.ICU.

You should then bring up the exported file to familiarize yourself with the different sections of the file. To do this enter the command:

E DOMAIN.ICU <ENTER>

As you begin to scan through the file, you will notice that the file is organized as a series of [LIST] and detail sections. The following section summarizes the different sections.

Before going on to the importer (BA.EXE), take some time to familiarize yourself with the output of the exporter. To rebuild an entire domain or just a part, you will only have to make a few minor changes to the output file so that it can be used by the importer (primarily changing "list" sections to add sections).

Export/Import ASCII File Format

The export/import utilities handle all the types of objects used within LAN Server including users, groups, aliases, applications, and access control lists. We have organized the file format so that you will find sections that provide overview of a particular class of object followed by the detailed sections that describe the specifics of each instance of an object. This organization is designed to give you an overall view (for navigation) followed by the detail information itself. The export utility will also provide you with summary information for each type of object provided as comments in the report.

When looking at the output of the export utility, much of the information (reference information) is not needed for import operations. We have dumped just about every piece of information that there is so that you have a complete picture of your domain. If this information appears in an import file, it will simply be ignored.

Object types include the following

Object Type	How is it used
[USER_..]	User and administrator accounts
[GROUP_..]	Define groups and assignments by group memberships
[APP_..]	Applications
[ALIAS_..]	Alias and shared resources (files, printers, and serial ports)
[ACL_..]	Permissions for resources (files, printers, serial ports, and named pipes)

For each object type you will see and use the following sections:

Section	Function
[.._List]	List and statistics of this type of object
[.._Add]	Objects to add
[.._Delete]	Objects to delete
[.._Update]	Objects to change

List Section

There are two purposes for the list sections. When exported, you will find summary statistics provided on what your current DCDB contains as comments in the output. The second purpose is to provide a list of the names of the objects so that their individual sections can be referenced. For example, in the [USER_LIST] section, if there is a user entry: USER=PHIL, then there should be a section called: [USER_PHIL] that contains the user information for setting up that user.

To add objects, you will need to change the list section from "[.._LIST]" to "[.._ADD]" and then run the import utility on the file. You will also need the customized sections referenced within "[.._ADD]" section unless the default properties for the to be created objects are sufficient.

Here is an overview of the different list sections:

Section Title	Function
[SERVER_LIST]	Shows the number of servers in the domain as well as their names and roles within the domain. This information is primarily informational -- you must set-up servers manually. Once set-up, you can then import the user, group, and ACL information via these utilities
[ALIAS_LIST]	Show the number of aliases in domain, their names, and comments
[USER_LIST]	Shows the count of users, user names, privilege, and comment
[GROUP_LIST]	Shows the count of groups, group names, and comment
[ACL_LIST]	Show the count of resources within the domain, their names and the server they are located on.
[APP_PUBLIC_LIST]	Shows a count of public applications, their names, and comments. Private applications are located immediately following each user's section that uses a private application.
[ALIAS_USER_XREF]	Report section providing a cross reference list showing the users assigned to each alias within the domain. Useful for finding missing aliases and for doing load balancing of resources.

Reference to LU.EXE Command Line Options

There are general rules regarding the use of command line options in the LU.EXE program. First, the normal setting for the program is to act as though the options for ALIAS, USERS, XREF, MODALS, BANNER, GROUPS, ACCESS are all enabled. If you select one or more of the foregoing options, the rest are turned off. This method of selecting single or multiple options is designed to make reporting as flexible as possible.

The order of parameters on the line is not important. Generally, only the first three letters of a report are needed. For example, you can select the alias option with "-ALI", or you can select users with the option "-USE". Of course, if the parameter requires a file name, the whole parameter must be typed in.

-[Q]uiet – turns off output to console only
Normally the output of the LU.EXE program goes to the display. If you are capturing the output of the program using the "-O" option, you may not want to see the identical output scroll on the screen. This option turns off the program's output to the screen.

-[V]erbose – provides additional status information
Some operations such as access control information retrieval can take extended periods of time to complete. This option allows you to see the progress of LAN operations. The details include the percentage completed (for operations of known scope), as well as general indications of progress using an animated text spinner on your console.

-[O:LOGFILE NAME] (To send report to file (append mode)
-[AO:LOGFILE NAME] (To send report to file (append mode)
This option allows you to capture the output of the program into a file. Note that the log file operates in an "append" mode; adding the output of each run to the end of the last. If there is no existing file of the name given in this parameter, the program will create it.

The output of the LU.EXE can be used as input to the other modules in the LAN Intensive Care Utilities package. This switch sets the name of the file that gets the captured data. The "AO" and "O" options do the same thing.

-[RO:LOGFILE NAME] (To send report to file (replace mode)
-[WO:LOGFILE NAME] (To send report to file (replace mode)
Operates like the previous "-O" option except it replaces the previous log file with a new one for the current run. You may want to use this option if you are using the LAN ICU package with REXX scripts where the logs are archived. The "RO" and "WO" options do the same thing.

-[ALI]AS Report
The alias report generates a complete list of all aliases (both internal and external) with all settings. There are three different types of aliases: file, printer, and serial. In version 3.0 (previous versions) external aliases exist to access resources on servers that are

external to the logged on domain. These external resources were shared using a CMD file.

Because the external alias CMD is so specific to the network configuration of a company, this file will need to be manually modified and transported from machine to machine to maintain cross-domain compatibility.

-[USE]ERS Report

This report displays all of the information about one or more users (you can limit the list using the "-UM option"). The normal report will display base user information, logon alias assignments, public logon assignments, and auditing information. You can add the encrypted password information by adding the "-PAS" or "-XPA" options to the command line.

-[UN:StartUserID],EndUserId -limits reports to a range of userids)

In this version we have introduced the ability to limit operations in the exporter and analyzer to only a selected group of users with the new command line switch of:

```
-unStartId,EndID
```

This option can be used a number of ways to limit the scope of your operations with these utilities. With this option you can select a single user or a range of users depending on where they are in the alphabetical list.

Selecting a single user

To select a single user, just enter the userid of the user as the sole parameter (no commas). For example, to just export the account called ACURLY using the rule file called RULE.ICU, you would enter the following command:

```
LU -i:RULE.ICU -un:ACURLY
```

Selecting a range of users

With this option you can limit the operations to a range of alphabetic characters. The first parameter specifies the starting name and the second parameter specifies the ending name. If neither name is the name of an actual user, their alphabetic value will be used.

For example, to export all of the user accounts start are in the range from "A" to "G" (last account is account G - account name GOPHER would not be included since it is greater than G), you would enter the following command:

```
LU -i:RULE.ICU -un:A,G
```

You can also write this as all of the accounts up to and including the letter G with the command:

```
LU -i:RULE.ICU -un:,G
```

You can also specify all of the accounts after a name or letter by just specifying the first argument with a comma. For example, to specify all of the account that occur after and including USERID, you would use the following command:

```
LU -i:RULE.ICU -un:USERID,
```

Selecting group(s)

Starting with version 1.3 the -UN: option now applied to group names also. If you wish to limit the groups listed, enter the group names as the user names for group information reports (-GROUP).

Control Access Control Entries Reports

The -UN option now limits the users listed in the -ACE report. Using this feature you can now export a specific user's access control information.

-[SER]VERS Report

This report shows you all of the on-line servers (as well as those that are currently off-line or missing from the domain, but not deleted). It also shows you the working parameters of each server. This is a useful report to determine how each of the servers has been configured.

-[APP]LICATIONS (Public) Report

The Applications report provides you with a complete list of public applications as well as the parameters for each application. Public application logon assignments are found in the "-USER" section.

-[XRE]F Cross reference Aliases and Users Report

This report shows the users that have logon assignments to each alias in the domain (including file, printer, and serial aliases).

A very important feature of this report is the display of "orphan" aliases. Orphan aliases are aliases that are referenced by user accounts, but do not exist on the LAN. This can be caused by an off-line server, or by the deletion of an alias before removing all references in user accounts. This report can help you cure the dreaded: "One of your logon aliases failed" at user login time. The analyze utility can be used to clear these also.

Starting with version 1.3, the logon device assignments are now listed in the cross reference report. This should prove useful in verifying that users are all assigned the same physical assignments.

-[BAN]NER Report

The banner information shows you the revision of the software. Also shown are the user and company name. Use this option to quickly check the version of software you are using.

-[MOD]ALS Report (System Security Policy)

LAN Server provides a domain-wide security policy of minimum/maximum password ages, as well as password history. These settings can be changed at the command line using the NET ACCOUNTS command. Due to a bug in LAN Server, these should be changed at the domain controller or via the NET ADMIN command if you wish to make the change remotely.

-[WOR]KSTATION Settings Report

This information shows you the current name of the logged on user (usually your userid) as well as the domain and domain controller server names. It also reports the heuristics in use. It is a good idea

to append this information to all reports to show where the data was extracted from and by whom.

–[GRO]UPS Report

This report displays the names of all groups within the system. It then provides a list of members within each group as well as the comment for each group.

–[ACC]ESS Control Report

This report is broken into two major sections. The first section displays all of the resources in the domain. The second report displays the resources and permissions by user and group. We call the first report the ACCESS or RESOURCE report. The second report is called the USER ACE and GROUP ACE report.

The first report is designed to show you all of the user and group permissions by resource name (or subdirectory name if a file alias is listed). In this version we break up server disks into drive letters and extract the resources by drive. In some cases you may get an error that there is more than 64K worth of data to be returned. In this case, you can use the "-RSRC" option to extract the drive in smaller subsections that are less than 64Kbytes.

–[BAD] ACLS Report–warnings about bad ACLs (builds FIXACLS.ACL)

The "-BAD" option checks for problems with ACLS. Empty ACLs and non-existent directories/files with resources are flagged. The program now generates a file: FIXACL.ICU that can used in the BA program to erase the bad entries. Each entry is annotated.

–[RSRC:]Server, Resource or Alias Name, Recursion(Y/N) (ACLs by server & path)

Allow you to selectively extract only a part of the access control list of a server. This feature is designed to speed the migration of access control information from one server to another.

Audit information is also extracted with each resource.

The resource parameter format is:

LU –RSRC:SERVER,RESOURCE,RECURSIVE

Where:
SERVER = Name of server such as **XYZ, ABC**

NOTE: Do not enter server names in the format:
\\XYZ or \\ABS

RESOURCE = The name of the subdirectory starting path for the resource(s) to be extracted.

For example: **C:\IBMLAN** will give you all of the subdirectories such as **C:\IBMLAN\DCDB,**
C:\IBMLAN\ACCOUNTS

NOTE: The **RECURSIVE** flag controls whether subdirectories below the **RESOURCE** path will be shown

NOTE: If the **RESOURCE** is given without the ending backslash, then names like **C:\IBMLANX, C:\IBMLANA** will be listed.

RECURSIVE = (Y/N) indicates whether to extract all subdirectories below the starting point given in **RESOURCE**. If you are extracting user subdirectories, then you want this set to **"Y"**es.

Important Note: The format of information on server access control lists has been changed with the 1.2 version of this program. You may need to recapture previous ACL information using the new exporter (LU.EXE) to use it in the importer (BA.EXE)

Example:

To extract all of the ACLs on server **"SRVPHIL"** for the subdirectories known as **C:\MAGNUM**, you would enter the following command:

LU -RSRC:SRVPHIL,C:\MAGNUM,Y -O:MAGNUM.ICU

This command also saves the resulting ACL lists in the file known as **MAGNUM.ICU**.

Alias Option on resource command:

Starting with version 1.4 you can retrieve the ACLS based on an alias name. For example, to extract the ACLS for the alias "ROOT_D", you would enter the following command:

LU -RSRC:,ROOT_D

When using the alias option, you do not need the server name, as this information is picked up from the alias definition.

-RSRC 64K limit lifted

Version 1.4 and above handles the case of more than 64K worth of data available for a resource path.

-RSRC Server Header Information Added

Version 1.4 and above creates a [Server_List] section and automatically adds this header information.

-[PAS]SWORD - Extract encrypted password plus user data
This feature adds the encrypted password with the normal user data. To enable this feature, add the "-PAS" (password) parameter. For example:

LU -PAS -USER

This command extracts all of the user information including the passwords.

The exported encrypted passwords can be imported by the import utility BA.EXE. To provide the most flexibility, the passwords can be moved using any workstation or by performing the action at the domain controller itself. The export and import operations are much faster if performed at the domain controller.

In this release you will find two modules: PWDEXP.EXE and PWDIMP.EXE--these files must be in the same directory as LU.EXE and BA.EXE for the password import/export feature to work.

This option adds the following line to the output file:

PASSWORD_ENCRYPTED=010203040506070809010111213141516

The data will vary depending on the password of the user.

IMPORTANT NOTE: Even though the password information is encrypted, you should still maintain tight control over this information. By comparing the encrypted information between users, it may be possible to figure out the password. For example, if two accounts have the password of "PASSWORD", the encrypted data would be identical.

-[XPA]SSWORD - Extract encrypted password exclusively
(no user data)
Sometimes you do not want all of the user data, just the passwords for the user or users. This limitation is accomplished with the "-XPA" (exclusive password). For example, to extract only the passwords use the command:

LU -XPA -USER

You can limit the user passwords by using the -UN option.   For example, to get the password for user "PL" only, enter the following command:

LU -XPA -USER -UN:PL

IMPORTANT NOTE: Even though the password information is encrypted, you should still maintain tight control over this information. By comparing the encrypted information between users, it may be possible to figure out the password. For example, if two accounts have the password of "PASSWORD", the encrypted data would be identical.

-[DOM:DOMAIN_NAME] (override logon domain name)
This parameter provides the administrator with cross domain administration capabilities. Without this parameter, the utility will operate only on the domain that the administrator has logged in to. With this parameter, you can operate on a domain other than the one logged in to.

For this feature to work, the userid and password must be identical between the logged-in domain, and the one specified in this argument.

-[SRV:SERVER_NAME] (override primary domain controller
name)
Normally the utilities within the LAN ICU package will use the server defined as the primary domain controller within the domain. This argument allows you to target another server within the domain. Possible targets include backup domain controllers.

```
-[ISRV:SERVER_NAME,SERVER_NAME...]
     Operate only on these servers

-[XSRV:SERVER_NAME,SERVER_NAME...]
     Exclude these servers
```

When accumulating information from a large domain, the amount of data can become enormous. To minimize the data, we have provided two commands: one to exclude certain servers (to exclude problematic servers), and another to specify the servers to export. Depending on your needs, you could use either of these commands.

```
- [ E{A,D,U} :

{[USE]ER,[GRO]UP,[ALI]IAS,[APP]LICATIONS,[ACL],[ACE],[ALL
]}
     - Change Export [List] sections to
       [Add],[Delete],or [Update] sections
```

Import DCDB & NET.ACC Info Without Editing

In this version you can change the header sections from [..._LIST] to ADD, UPDATE, or DELETE sections using the new -E option. The next letter after -E stands for the type of section(s) to generate. A=ADD, D=DELETE, U=UPDATE. This is then followed by a colon followed by the type of resource section to change. The resource names are: [USE]ER, [GRO]UP, [ALI]IAS,[APP]LICATIONS,[ACL],[ACE],[ALL].You can use more than one option at a time. The ALL option changes all sections that are generated.

For example, to change the user export from a list to an ADD, you would enter the command:

> -EA:USER

To change the ACE entries from LIST to UPDATE, you would use the command:

> -EU:ACE

For example, to refresh the access permissions for the user "PHIL" with the file REFRESH.ICU you would use the following command to create the change file:

> LU -ACE -UN:PHIL -EU:ACE -V -O:REFRESH.ICU

To then apply this newly created file, you would use the command:

> BA -I:REFRESH.ICU

```
-[F]{[F]ile, [D]irectory, [N]on-existent, [P]rint,
[C]omm, p[I]pe} ACL filter
```

Filtering ACLs for only files/directories etc.

One of the most requested features for ACLs was the ability to filter the output of the ACL report to just files or directories. This has been accomplished with a new command line switch in the LU.EXE program. The

31

'-F:' or filter switch takes any single or combination of letters as follows to control the filtering of ACLs:

```
F - Files
D - Directories
N - Non-existent directories (seen on FAT only)
P - Printers
C - Communications (Serial ports)
I - Pipes
O - Others (anything other than the above)
```

For example, to just list the files with ACLs on a domain, enter:

```
LU -ACL -F:F
```

To list the printers, communnciation ports, and pipes, enter the following:

```
LU -ACL -F:PCI
```

The filter will also affect the ACE reporting; only showing those users that have ACEs that meet the filter criteria.

If you do not supply a filter parameter, the default of ALL is assumed.

```
-[BUF1] Buffer one directory entry only (default)
-[BUF3] Buffer three directory entries
-[BUF64] Buffer 64K of directory entries
```

Controlling Buffer Size

When accessing directory entries from remote servers that have large drives, you can control the buffering of entries. You can buffer 1, 3 or 64K worth of directory entries. When accessing a LAN Server 3.0 domain with HPFS-386 from an LAN Server 4.0 requester, only the 1 entry buffer should be used (bug in LAN Server 4.0)--this is the default. In other cases you can use the larger buffer size.

Chapter 3 - Batch Editor Overview (BA.EXE)

Overview of Batch Editor operation

Before using the batch editor, you should be familiar with the output of the exporter (LU.EXE). Using the batch editor is very simple: you simply modify the output file from the exporter so that the LIST sections become ADD, DELETE, or UPDATE sections. Because one thing depends on another within the domain, the batch editor processes the sections of the file in a specific order as follows:

1) Group names sections
2) Aliases
3) Public Applications
4) Users
5) User Passwords
6) Group membership (users) sections
7) Access Control Entries (ACEs) for users and groups

Within each section, operations are performed in the following order:

1) Delete
2) Add
3) Update (not all sections have updates)

The order of sections and operations within the batch editor input file is not important. The utility will search through the file looking for appropriate sections in the aforementioned order. The editor will not generate any errors for sections that do not exist. Consequently, you can put as little or as much as you like within the editor's input file and in any order you wish.

The reason for this ordering is a result of the reference order of the LAN. For example, you cannot add a user to a group if that group does not exist. You cannot assign a logon assignment to an alias before it exists. Similarly, you cannot assign a public application to a user before that application exists. So the order of sections is strictly the result of the need for resources to be in place before users are created.

Trying out the importer for the first time

To see the command line options of the exporter, try the following command:

BA ? <ENTER>

You should then see the following output:

```
BA.EXE Batch Editor (version 951228)
     -syntax:  BA [switches] [-O:LOGFILE]
 'LAN Intensive Care Utilities' for IBM LAN Server
  Copyright 1994,1995,1996 - Lieberman and Associates
       Design and Engineering Group

 -I:Input_Command_file_name (Source file for batch editor)
 -[O:]Output_log_file_name (Send report to file (append))
 -[AO:]Output_log_file_name (Send report to file (append mode))
 -[RO:]Output_log_file_name (Send report to a file (replace
mode))
 -CN:OldName,NewName (rename a user for user Add/Delete/Update)
 -[Q]uiet - kills output to terminal
 -[ALI]AS Processing
 -[USE]ERS Processing
 -[APP]LICATIONS (Public) Processing
 -[GRO]UPS Processing
 -[ACC]ESS (ACE+ACL) Processing
 -[ACE] User/Group Processing
 -[ACL] Resource Processing
 -[MEM]BERS of Groups Processing
 -[BAN]NER Display
 -[E{A,D,U}:{[USE]ER,[GRO]UP,[ALI]IAS,[APP]LICATIONS,
      [ACL],[ACE],[ALL]}
   Change Export [List] sections to [Add],[Delete],or
      [Update] sections
 -[DOM:DOMAIN_NAME] (override logon domain name)
 -[SRV:SERVER_NAME] (override primary domain controller
      name)

 Default settings are all sections are processed and reports to
console. Selecting any one section processing, disables the rest
unless they are also selected on the command line.  You may put
the parameters in any order you wish.  Capitalization is not
important.

 Default input command file name: 'DOMAIN.ICU'
```

The importer uses two files for its operation: an input command file and an audit log file (optional). The input command file contains the modified output from the exporter. This is the file that is used to build and modify your domain. The input command file must be supplied, otherwise the importer will attempt to use the default input file known as: "DOMAIN.ICU".

The second file is an optional output log file that captures the operation results of the program into a disk file. This is an important

file since it creates a permanent record of all changes you make to the domain. If you use the same log file name over and over again, each run of the exporter will be appended to the end the file. This second file is an audit file that maintains a copy of everything you see going by on the screen.

We have put together a few samples to help you learn about the importer and how it works. The samples file we will use are known as STOOGES.ICU and NOSTOOGE.ICU. The first file demonstrates how to add groups, users, and memberships to groups. The sample also uses templates to make the set-up easier.

Here is the listing of the STOOGES.ICU file on your disk:

```
;LAN ICU Batch Input File:
;     STOOGE.ICU
; Creates the created demo groups and users
;
; * * * *  G R O U P S * * * *
;Delete the demo group to start
[GROUP_DELETE]
 GROUP=STOOGES
 GROUP=STURGEON

;Next, add them in (no members on create)
[GROUP_ADD]
 GROUP=STOOGES
 GROUP=STURGEON

;Details for added groups
[GROUP_STOOGES]
Comment=This is the stooges group
member=amoe
member=acurly
member=alarry  ;Another comment

;This is another group
[GROUP_STURGEON]
Comment=This is the genius group

;Add the members into STOOGES group at end
[GROUP_USER_ADD]
group = stooges      ;hi
```

(Continued on next page)

```
; * * * *   U S E R S * * * *
; Delete the demo users to begin
[USER_DELETE]
  user = AMOE   ;comment
  user = ALARRY
  user = ACURLY

;Now add in the members using BOSS and KNUCKLEHEAD
; templates
[USER_ADD]
 user_BOSS=AMOE,STOOGE1,Hi,I'm MOE-the first stooge
 user_KNUCKLEHEAD=ALARRY,STOOGE2,Hi, I'm LARRY-the second
stooge
 user_KNUCKLEHEAD=ACURLY,STOOGE3,Hi, I'm CURLY-the third
stooge

; Only special thing about BOSS is that it is
; and administrator.
[USER_BOSS]
Privilege=ADMIN

; And there is nothing special about KNUCKLEHEAD
[USER_KNUCKLEHEAD]
Privilege=USER
```

As the first operation, let's create the groups known as "Stooges" and "Sturgeons". To do so, execute the following command:

BA –I:STOOGES.ICU –O:STOOGE.LOG –GROUP <ENTER>

You should see the Batch Editor respond back with the messages indicating that these groups were not deleted because they currently do not exist. Next you will see a message indicating success in the creation.

Next, let's create the user accounts for Moe, Larry, and Curly. Notice that Moe has been made an administrator, while the other two are regular users. This was done by using the templates known as "BOSS" for Moe, and "KNUCKLEHEADS" for Larry and Curly. To add the users, execute the following command:

BA –I:STOOGES.ICU –O:STOOGE.LOG –USER <ENTER>

NOTE: Do not worry about the accounts just created. We will erase them at the end of the tutorial.

The final step we will take in this simple tutorial will be to add the just created members to the 'stooges' group. To do so, execute the following command:

BA –I:STOOGES.ICU –O:STOOGE.LOG –MEMBERS <ENTER>

At this point you have seen how to selectively activate sections from the STOOGES.ICU file. You can execute the entire series of adds, deletes, and updates in one shot. To do this, execute the following command:

`BA –I:STOOGES.ICU –O:STOOGE.LOG <ENTER>`

By not specifying the restrictions, you can see all operations being performed.

Getting rid of the demo accounts

To remove the just added groups and users, we have provided the following script known as "NOSTOOGE.ICU":

```
;LAN ICU Batch Input File:
;    NOSTOOGE.ICU
; Deletes the created demo groups and users
;
; * * * *  G R O U P S * * * *
;Delete the demo group to start
[GROUP_DELETE]
 GROUP=STOOGES
 GROUP=STURGEON

; * * * *  U S E R S * * * *
; Delete the demo users to begin
[USER_DELETE]
  user = AMOE   ;comment
  user = ALARRY
  user = ACURLY
```

To delete the demos, enter the following command:

`BA –I:NOSTOOGE.ICU –O:STOOGE.LOG <ENTER>`

Congratulations, that's how simple it is to add and delete groups and users.

If you already have a LAN in place (with all of the needed resources in place) and want to add users quickly, jump to the section entitled: "Adding User Accounts."

The following section summarizes some of the different types of sections you will be creating when working with the Batch Editor/Importer.

ADD Section

When you are ready to add to your domain, you will need to create the appropriate ADD sections. You must first list the names of the new entries, followed by the sections with these new names.

Section Title	Function
[USER_ADD]	Names of users to add. You must create a user section for each name.
[GROUP_USER_ADD]	Uses group detail sections to derive list of members to add to a group
[GROUP_ADD]	Names of groups to add. You must create a group section with member list. Groups should be created before users are added. In this utility you can provide application and alias assignments as part of the group memberships. The importation utility will automatically add in the assignments when user account is created. The ANALYZE utility can also use this group information to confirm the proper assignments for all users in the domain.
[APP_ADD]	Names of public applications to add.
[ALIAS_ADD]	Names of aliases to add. You must create an alias section for each of the names in this section.

Update Section

In some cases you may not have to create a new account or alias, but just modify one or more of the settings of an object. This section allows you to make just adjustments to an existing object.

Section Title	Function
[USER_UPDATE]	Names of users to update. You must normally create a user section for each name. However, may also do updates by using a template.
[GROUP_UPDATE]	Allow you to change the comment on a group.
[ALIAS_UPDATE]	Names of aliases to update. You must create an alias section for each of the names in this section.

Section Title	Function
[USER_DELETE]	List of user names to delete
[GROUP_DELETE]	List of groups to delete
[GROUP_USER_DELETE]	List of group sections containing memberships to delete.
[ALIAS_DELETE]	List of aliases to delete
[APP_DELETE]	List of public applications to delete

Reference to BA.EXE Command Line Options

There are a few general rules regarding the use of command line options used in the BA.EXE program. First, the normal setting for the program is to act as though the options for ALIAS, USERS, BANNER, GROUPS, ACCESS are all enabled. If you select one or more of the foregoing options, the rest are turned off. This method of selecting single or multiple options is designed to make operation as flexible as possible.

The order of parameters on the line is not important. Generally, only the first three letters of a report are needed. For example, you can select the alias option with "-ALI", or you can select users with the option "-USE". Of course, if the parameter requires a file name, the whole parameter must be typed in.

`-[Q]uiet - turns off output to console only`
Normally the output of the BA.EXE program goes to the display. If you are capturing the output of the program using the "-O" option, you may not want to see the identical output scroll on the screen. This option turns off the program's output to the screen.

`-[O:LOGFILE NAME] (To send report to file)`
`-[AO:LOGFILE NAME] (To send report to file (append mode)`
This option allows you to capture the output of the program into a file. Note that this option operates the log file in an "append" mode; adding the output of each run to the end of the last. If there is no existing file of the name given in this parameter, the program will create it.

It is a good idea to always have a defined log file to audit all operations.

`-[RO:LOGFILE NAME] (To send report to file (replace mode)`
`-[WO:LOGFILE NAME] (To send report to file (replace mode)`
Operates like the previous "-O" option except it replaces the previous log file with a new one for the current run. You may want to use this option if you are using the LAN ICU package with REXX scripts where the logs are archived. The "RO" and "WO" options do the same thing.

`-[CN:OldName,NewName] (Rename a user for user`
`Add/Delete/Update`
If you have ever wanted to rename a user without editing the export file, this is the command for you. The idea behind this command is simple. First, export a single user by name using the -UN: option. Next, use the -E option to affect how the user information is to be used (Add/Delete/Update). Use this switch to affect the user name specified. For example, to delete the user called ACURLY and rename him as ASHEMP, you would use the following commands:

```
LU -UN:ACURLY -USER -O:ASTOOGE.ICU
        (Exports ACURLY)
BA -ED:USE -i:ACURLY.ICU
        (Deletes the ACURLY Account)
```

```
          BA -EA:ALL -i:ACURLY.ICU -CN:ACURLY,ASHEMP
                    (Creates ASHEMP from ACURLY)
```

This method allows you to change a user's identity, while retaining the rest of the user's account.

`-[ALI]AS Processing`

This option causes all alias sections to be processed (both internal and external). There are three different types of aliases: file, printer, and serial. In version 3.0 (previous versions) external aliases exist to access resources on servers that are external to the logged on domain. These external resources were shared using a CMD file.

Because the external alias CMD is so specific to the network configuration of a company, this file will need to be manually modified and transported from machine to machine to maintain cross-domain compatibility.

`-[USE]ERS Processing`

This option processes all of the user information sections.

`-[APP]LICATIONS (Public) Processing`

The Applications Processing provides you with a complete list of public applications as well as the parameters for each application. Public application logon assignments are found in the "-USER" section.

`-[BAN]NER Display`

The banner information shows you the revision of the software. Also shown are the user and company name. Use this option to quickly check the version of software you are using.

`-[GRO]UPS Processing`

This option processes the group sections. Note that groups are processed in a two part process. First the groups are created. After all user accounts have been processed/added, members can be added.

`-[ACC]ESS Control Processing`

This Processing is broken into two major sections. The first section processes the resources in the domain. The second phase processes the ACEs by user and group.

`- [ E{A,D,U} :`

```
{[USE]ER,[GRO]UP,[ALI]IAS,[APP]LICATIONS,[ACL],[ACE],[ALL
]}
    - Change Export [List] sections to [Add],[Delete],or
[Update]
       sections
```

Import DCDB & NET.ACC Info Without Editing

In this version you can change the header sections from [..._LIST] to ADD, UPDATE, or DELETE sections using the new -E option. The next letter after -E stands for the type of section(s) to generate. A=ADD, D=DELETE, U=UPDATE. This is then followed by a colon followed by the type of resource section to change. The resource names are: [USE]ER, [GRO]UP, [ALI]IAS,[APP]LICATIONS,[ACL],[ACE],[ALL].You can use more than one option at a time. The ALL option changes all sections that are generated.

For example, to change the user export from a list to an ADD, you would enter the command:

    -EA:USER

To change the ACE entries from LIST to UPDATE, you would use the command:

    -EU:ACE

For example, to refresh the access permissions for the user "PHIL" with the file REFRESH.ICU you would use the following command to create the change file:

    LU -ACE -UN:PHIL -V -O:REFRESH.ICU

To then apply this newly created file, you would use the command:

    BA -I:REFRESH.ICU -EU:ACE

– **[DOM:DOMAIN_NAME] (override logon domain name)**
This parameter provides the administrator with cross domain administration capabilities. Without this parameter the utility will operate only on the domain that the administrator has logged into. With this parameter, you can operate on a domain other than the one logged into.

For this feature to work, the userid and password must be identical between the logged-in domain, and the one specified in this argument.

– **[SRV:SERVER_NAME] (override primary domain controller name)**
Normally the utilities within the LAN ICU package will use the server defined as the primary domain controller within the domain. This argument allows you to target another server within the domain. Possible targets include backup domain controllers.

43

Chapter 4 - Batch Editor: User Accounts

Overview

You can perform adds, deletes and updates of users on you domain with the information in this section. The unique capability of the update operation is to retain your users' passwords and to only change those parameters that appear in the user's detailed section.

Deleting users is as simple as putting their names in a section called [USER_DELETE]. Adding users is almost as simple. To add users you create a [USER_ADD] section where you insert the names of the users to create. There is a template based creation method that only asks you for the unique userid, password and comment of each user. If you are adding a user from another domain, you can use the detail sections created from that domain (remember that you must purchase a copy of LAN Intensive Care Utilities for each domain the package acts on). The only unique item that must be entered when transferring users from one domain to another is the user's password. Finally, updating user accounts is almost the same as adding user accounts except a [USER_UPDATE] section is used. With an update section, you only need to enter parameters that have changed into the user's detail section.

Deleting User Accounts

To delete users, you will have to create entries in a [USER_DELETE] section. The entries in the [USER_DELETE] section appears as follows:

USER=**USERID**

or

ADMIN=**USERID**

where:

USERID - this is the user name for the user to delete

Example:

```
[USER_DELETE]

     user=JBEAMIS
     user=KFUN
;  user=PLIEBE
;  user=FRODRI
```

In this example, we have deleted two user accounts: JBEAMIS and KFUN. The entries for PLIEBE and FRODRI are not deleted since they are commented out in the delete section.

HINT! If you are planning to move users from one domain to another, you will use this [USER_LIST] section from the original domain as basis for the [USER_DELETE] operation as well as the basis for the [USER_ADD]. By using comments ";" on lines you want to ignore, you can include the entire list section and just comment out those entries you do not want action on.

Adding User Accounts - Overview

You can add users via two methods:

1) Reference a complete named user section (using the direct output of LU.EXE)
2) Using a template or example account and then just specify a unique USERID, PASSWORD, and COMMENT for that user. Use this method for adding groups of new users.

Both methods are very simple to do.

Adding Users - Complete Reference Section Method

To create a unique user, you will have to create an entry in the [USER_ADD] section and then create a complete user reference section to match. The entry in the [USER_ADD] section appears as follows:

USER=**USERID**

or

ADMIN=**USERID**

where:

USERID - this is the user name for the new user

Example:

```
[USER_ADD]
      user=JBEAMIS
      user=KFUN
    ; user=PLIEBE
    ; user=FRODRI

[USER_JBEAMIS]
  User_Comment= Jerry Beamis - X1658 Tower
  Full_Name=Jerry Beamis Sr. VP
  Comment=PS2 model 95
  Password=JIMMY
  Account_Active=YES
      *
      *
[USER_KFUN]
  User_Comment=Kim Fun - X1926 Tower
  Full_Name=Kim Fun Sr. VP
  Comment=PS2 model 295
  Password=HAPPY
  Account_Active=YES
      *
      *
```

In this example, we have created two accounts for userid's JBEAMIS and KFUN. All of the public/private application assignments, group memberships, logon alias assignments, as well as all other settings must be entered in each user's section. The entries for PLIEBE and FRODRI are ignored since they are commented out.

HINT! This method is normally used when recreating the domain or when moving users from one domain to another. The easiest way to move users from one domain to another is to first export all of the user to a file, change the [USER_LIST] section title to [USER_ADD], and finally comment out the users that you do not want added as part of the import process.

You can add as many users as you wish. The total number of users within a domain is limited solely by LAN Server (the maximum is 1895 users in LAN Server 3.0).

Adding Users -Template Method (quick method)

To create a user via the template method you will need to create a special type of entry line in the following format in the [USER_ADD] section:

USER_**TNAME**=**USERID,PASSWORD,COMMENT**

where:

TNAME - the name of a user section within the batch file that will be used for setting up the new user account. The template user account will be searched for both private and public application assignments, alias logon assignments, as well as all of the other settings.

USERID - this is the user name for the new user
PASSWORD - this is the initial password for the user
COMMENT - this is a user comment for the account

Example:

```
[USER_ADD]

    user_exec=JBEAMIS,JIMMY,Jerry Beamis - X1658 Tower
    user_exec=KFUN,HAPPY,Kim Fun - X1926 Tower


[USER_EXEC]
  User_Comment=This is an executive template account
  Full_Name=
  Comment=Default comment for EXEC
  Password=
  Account_Active=YES
    *
    *
    *
```

In this example, we have created two accounts for userids JBEAMIS and KFUN based on the template known EXEC. All of the public/private application assignments, group memberships, logon alias assignments, as well as all other settings are inherited from the template account.

HINT! The easiest way to create the template accounts is to run the exporter (LU.EXE) and use one or more of the existing user account sections. You can copy a section and rename it to something else if you wish.

HINT! You do not have to supply all of the parameters on the line if you wish the account to pick up parameters from the template. For example, if you just want to pickup everything from template, you can enter:

user_exec=JBEAMIS

If you want to supply the name and comment, but have the password come from the template, just enter the following:

```
user_exec=JBEAMIS,,Jerry Beamis - X1658 Tower
```

Finally, if you want to just provide the name and password, but want the comment to come from the template, enter the following:

```
user_exec=JBEAMIS,JIMMY
```

You can provide as many templates as you wish and create as many users as you wish. The total number of users within a domain is limited solely by LAN Server (the maximum is 1895 users in LAN Server 3.0).

Updating Users - Complete Reference Section Method

To update a user without using a template, you will have to create an entry in the [USER_UPDATE] section and also create a complete user reference section to match. The entry in the [USER_UPDATE] section appears as follows:

USER=**USERID**

or

ADMIN=**USERID**

where:

USERID - this is the user name for the user account to update

Example:

```
[USER_UPDATE]

      user=JBEAMIS
      user=KFUN
   ; user=PLIEBE
   ; user=FRODRI


[USER_JBEAMIS]
  User_Comment= Jerry Beamis - X2001
  Full_Name=Jerry Beamis President
  Comment=PS2 model 95
  Password=JIMMY
  Account_Active=YES
      *
      *
      *

[USER_KFUN]
  User_Comment=Kim Fun - X1700  Tower
  Full_Name=Kim Fun  Sr. VP
  Comment=PS2 model 295
  Password=HAPPY
  Account_Active=YES
      *
      *
      *
```

In this example, we have updated two accounts for userids JBEAMIS and KFUN (revised comments and full names). All of the public/private application assignments, group memberships, logon alias assignments, as well as all other settings are carried forward if there were no new values in each user's section. The entries for PLIEBE and FRODRI are ignored since they are commented out.

Fast updates of large groups of users and assignments

When you are not sure that all users of a group have the proper assignments, you can create a template sample section that contains all of the proper assignments. You can then refer to the entries in an [UPDATE_USER] section. The accounts will be refreshed based on the example template you supply. Be careful though; only put in those parameters that need to be the same between groups. If you inadvertently put a password in the template (prototype), all of the users in your update list will get the same new password.

Please examine the following example to see how this is implemented:

```
[USER_UPDATE]

; All of the listed users will also get the changes in
; the [USER_STOOGES] section

; AMOE will get the new password: 'BOSS' and the
; new comment: 'Leader of the Stooges'

    user_stooges = AMOE,BOSS,Leader of the Stooges

; ALARRY will not get a new password (empty field),
; but will get the new comment: ``Crazy Hair''

    user_stooges = ALARRY,,Crazy hair

; ACURLY will get a new password

    user_stooges = ACURLY,WHOOP

[USER_STOOGES]
; Delete group membership in Genius
; & Add membership in Knucks

    Add_Member_of=Knucks
    Del_Member_of=Genius

; Add logon alias assignments for X & Y
; & delete assignments for Z

      Add_Logon_Asn=FILE:X:ROOT_C
      Add_Logon_Asn=FILE:Y:ROOT_D
      Del_Logon_Asn=FILE:Z:ROOT_E

; Add OS/2 AMIPRO & delete DOS WS from public apps folder

    Add_AppSel=OS2_PUBLIC:AMIPRO
    Del_AppSel=DOS_PUBLIC:WS

(continued on next page)

; Force user to change their password on next logon

    Password_Age = EXPIRED
```

User Reference Section

Sample User List Section

```
; User node memory space required: 363
; Group node memory space required: 528

[USER_LIST]
; Total # of Users=11

  Guest=GUEST  ;System ID
  User=SRVPHIL ;System ID - Server
  Admin=A1     ;Hi - I'm another comment
  User=NEWUSER
  Admin=USERID ;Default User ID
  User=SRVICS  ;System ID - Server
  User=X10
  Admin=PL
  User=X1
  User=X2
  Admin=U01
```

Sample User Detail section

```
[USER_PL]
  User_Comment=This is Phils Account
  Full_Name=Philip Lieberman
  Comment=Reference account
  Password=
  Account_Active=YES
  Account_Deletable=YES
  Password_Required=NO
  Password_Changable=YES
  Password_Age= 64 Days 4:55:00
  Privilege=ADMIN
  Logon_Script=YES
  Script_Path=
  Home_Dir_Required=NO
  Home_Dir=
  Operator=
  Application_Parms=
  Workstations=
  Account_Expires=NEVER
  Max_Storage=UNLIMITED
  Logon_Hours=ALL
  Logon_Server=\\*
  Country_Code=0
  Code_Page=437
  Logon_Asn=FILE:X:ROOT_C
  Logon_Asn=FILE:Y:ROOT_D
  Logon_Asn=FILE:Z:ROOT_E
  Member_of=ADMINS
  AppSel=OS2_PUBLIC:INSTPATH
  AppSel=DOS_PUBLIC:LANMSG
  Last_Logon=Tue May 17 14:55:48 1994
  Last_Logoff=Sat May 14 20:59:07 1994
  Bad_Password_Count=0
  Number_Logons=30
```

Key to User Detail Section Contents

Entry	Explanation
`[USER_name]`	This is the first line in the definition section of a user or administrator's account. This type of section is used for adding or updating a user account. **Syntax:** **[USER_** - Definition of user detail section *name]* - Name of user **Notes:** *This name must first appear in a LIST, ADD, DELETE or UPDATE section*
`User_Comment`	This is an optional comment section for the user's account. It can be up to 48 characters in length. This is the comment field you set in the full screen interface. **Notes:** The user comment field also appears in the list summary area as a comment on the line (;comment...). No quotes are needed for any comment field.
`Full_Name`	This is another comment field of up to 48 characters in length. It can contain the full user name or any other information you wish. This field is normally set by the command line interface.
`Comment`	This is another comment field of up to 48 characters in length. It can contain additional comments you wish. This field is normally set by the command line interface.
`Account_Active`	**Value:** **YES** - User may log on* **NO** - User account not available for log on **Notes:** Can be used to temporarily disable a user's account
`Account_Deletable`	**Value:** **YES** - Account may be deleted* **NO** - Account may not be deleted **Notes:** This setting allows you to lock accounts against accidental deletion by UPM.

`Password_Required`	**Value:** **YES** - User must supply valid password to log on* **NO** - No password required for log on **Notes:** This controls the level of security in your domain per user. You may not want to place a required password for the GUEST account.
`Password_Changable`	**Value:** **YES** - User may change their password **NO** - Password may only be changed by administrator **Notes:** This is a security and auditing issue.

`Password_Age`	Age of current password represented in days and HH:MM:SS.
	
	To force the user to change their password on their next logon, use this entry:
	        `Password_Age=EXPIRED`
	
	To reset the password change timer to 0 (maximum time to change password) use this entry:
	        `Password_Age=RESET`
	
	All other values for Password_Age are ignored.
	
	Before an account can be forced to change their password, you must set the maximum password age with the following command:
	NET ACCOUNTS /MAXPWAGE:DAYS

`Password`
 	
`[IMPORT only]`
	Initial password for this user's account.
	
	Notes:
	You should probably set the Password_Expires=YES so that the user must change their password on their first logon. This is a normal security precaution unless passwords are assigned and fixed by the system administrator.

`PASSWORD_ENCRYPTED`	Encrypted data created using the -PAS or -XPAS option exporter: LU.EXE. This field can be used for import and export operations for password synchronization.

`Privilege`	**Value:**
	  USER - User level privilege*
	  GUEST - Guest account (unknown name)
	  ADMIN - Administrator (all privileges)
	
	Notes:
	Operator privileges can be added to the USER account to give it additional capabilities, but not all of the administrator privileges. Do not give ADMIN level users any operator privileges as these will damage the account (by default ADMIN has all privileges already).

`Logon_Script`	**Value:**
	  YES - Specifies that a logon script is used*
	  NO - No logon script to use
	
	Notes:
	This is normally set to YES even if no Script_Path is provided.

`Script_Path`	The path name of the user's logon script (.CMD, .EXE, .BAT, or .PRO file). It can have no extension at all. If the file has no extension, it is assumed to be a .CMD or .BAT file. A blank entry in this field mean no logon script exists. The script path must be specified relative to the Netlogon service SCRIPTS path. An example of this line in IBMLAN.INI follows: SCRIPTS = C:\IBMLAN\REPL\IMPORT\SCRIPTS **Note**: you may imbed the userid as part of the path name by using the '%U' entry in the path. This allows you to customize standard templates.

Home_Dir_Required	
	Value: **YES** - Account must have a valid home directory for logon **NO** - Home directory is optional*
Home_Dir	This entry allows you to define a directory on the server to be automatically assigned at logon of this user. There are two formats for the setting: explicit drive letter assignment and automatic drive letter assignment (workstation drive letters). Explicit assignment format: **x:\machineID\Y$\pathname** where: **x**: = workstation drive letter to use **\machineID** = server name that holds the home directory **\Y$** = drive letter on server that holds home directory **\pathname** = remaining path to home directory on server Automatic drive assignment format (first free drive letter): **\\machineID\Y$\pathname** where: **\machineID** = server name that holds the home directory **\Y$** = drive letter on server that holds home directory **\pathname** = remaining path to home directory on server **Note:** To assign the root of the server, leave off \pathname from either of the methods above. **Note**: You may imbed the userid as part of the path name by using the '%U' entry in the path. This allows you to customize standard templates.

Operator	**Value:**
	   PRINT = print operator privilege is enabled.
	   COMM = comm operator privilege is enabled.
	   SERVER = server operator privilege is enabled.
	   ACCOUNTS = accounts operator privilege is enabled
	
	Notes:
	Multiple entries can be placed on the same line with commas in between. Please do not assign any of these operator privileges to an account that is an administrator. Doing so will cause the administrator privileges to be reduced--to restore privileges, you will need to delete the account and recreate it (no fun).

Application_Parms	Application parameters
Workstations	List of requester addresses from which a user is permitted to log on. A blank string means all requesters are allowed. (To disallow logon, the account disabled flag must be set.) Up to eight requesters may be specified. The list of requesters can include IBM NETBIOS permanent names, which are listed as machine IDs, consisting of 12 hexadecimal characters. IBM NETBIOS permanent names are entered in the requester as follows: 16DF.02AC.7DE9 with commas between 12 digit address entries.

Account_Expires	**Value:**
	   NEVER = No expiration date*.
	   DATE TIME (Not implemented Yet)
	
	Notes:
	Once the date and time have been reached, the account will change to Account_Active=NO.

Max_Storage	**Value:**
	   UNLIMITED = No limit to storage space for user*.
	   SIZE = Size in Kbytes
	
	Notes:
	In version 3.0 of LAN Server, this value is not enforced. To check if the user has exceeded their memory allocation, you can run the LAN Server CHKSTOR program.
	
	In version 4.0 of LAN Server this value is enforced.

Logon_Hours	Not completely implemented for importing in this version. Setting is reported completely. Import of value 'ALL' is supported in the current version.
Logon_Server	Server to use for log on. The entry of "*" signifies the primary domain controller (normal default). If you wish to spread out the log-on loading, you can specify the name of a secondary server that contains a replica of the domain control database (DCDB).

`Country_Code`	This is the OS/2 country code for the user's language choice. This is used by the LAN Server software to generate messages in the appropriate language whenever possible. Value is generally the international country code for telephone calls. Value of zero will default to language of LAN Server version in use.
`Code_Page`	This is the code page for the user. Normal default is 437 (multilingual Latin).

`Logon_Asn`
 	
`Example:`
`Logon_Asn=`
`FILE:X:ROOT_C`
	Log on assignments.
	This line allows you make LAN alias assignments to local drive letters on the user's workstation. If an asterisk '*' is entered instead of a drive letter, the first available free drive will be used instead. This command is equivalent to a NET USE command performed at logon.
	
	The syntax is as follows:
	 Logon_Asn=
	 `FILE:DRIVEID:ALIAS` for Files
	 `PRINTER:PORTID:ALIAS` for Printers
	 `SERIAL:COMID:ALIAS` for Serial
	
	where:
	`DRIVEID:  A:..Z:, or *`
	`COMID: COM1:..COM9`
	`PRINTERID: LPT1:..LPT9`
	
	 `ALIAS = Defined domain alias`
	
	You can have multiple "Logon_Asn=" assignment lines. You cannot use physical peripheral names of devices that actually exist on your machine.

`Member_of`	Group membership(s) for this user. You can have multiple "Member_of=" lines--one for each group membership. When you run the analyze utility as well as the import utility, this membership information will be used to setup the public applications as well as the alias logon assignments.

`AppSel`
 	
`Example:`
`AppSel=`
`OS2_PUBLIC:INSTPATH`
	Defines applications to populate the public and private applications folders for the user. You can have multiple line of AppSel= where each line represents a different public or private application within a folder.
	
	Format:
	`AppSel=APPTYPE:APPNAME`
	
	Where:
	APPTYPE can be:
	  OS2_PUBLIC
	  OS2_PRIVATE
	  DOS_PUBLIC
	
	APPNAME can be:
	any defined public or private application.
	
	Public applications are defined by sections that titled:
	[APP_PUBLIC_APPNAME]
	Private application sections are defined by userid as:
	[APP_PRIVATE_USERID_APPNAME]

`Init_DCDB=YES`	Initialize the DCDB files for a user. This entry is added by the Analyzer program when it detects an account that was set-up without logon assignments (Alias & Program).
`Fix_App_DCDB=YES`	Repair the DCDB for a user when an inconsistency was detected by the Analyzer program. If this line is executed, the DCDB is analyzed and fixed automatically.
`Sync_DOS_DCDB=YES`	Synchronize the OS/2 DCDB with the DOS DCDB logon files This entry is added by the Analyzer program when it detects these files are out of synchronization.

Last_Logon	This field provides you with the last date and time of logon for this user. For reference only. This is not a modifiable field.
Last_Logoff	This field provides you with the last date and time of logoff for this user. For reference only. This is not a modifiable field.
Bad_Password_Count	This field gives you the number of bad logon attempts for this user. For reference only. This is not a modifiable field.
Number_Logons	This field gives you the number of successful logons by this user. For reference only. This is not a modifiable field.

Chapter 5 - Batch Editor: Aliases

Deleting Aliases

To delete aliases, you will have to create entries in a [ALIAS_DELETE] section. The entries in the [ALIAS_DELETE] section appears as follows:

```
FILE = FILE_ALIAS_NAME    ;File alias to delete

PRINTER=PRINTER_ALIAS_NAME     ;Printer alias to
delete

SERIAL = SERIAL_ALIAS_NAME     ;Serial alias to
delete
```

Where:

```
 PRINTER =  Printer alias type
  FILE = File alias type
 SERIAL =  Serial alias type
```

Example:

```
[ALIAS_DELETE]

    printer=LJET15
    file=APPS_H
    serial=MODEM5
;   file=APPS_J
```

In this example, we will delete the printer alias LJET15, file alias APP_H, and serial alias MODEM5. Since the APPS_J alias was commented out, this will not be deleted.

Adding Aliases

In version 3.0 of LAN Server, there are both internal and external aliases. Internal aliases are located on the domain. External aliases are resources that are located on servers outside the domain. External aliases can be created by the LAN ICU package. However, you are responsible for writing a batch file to connect and disconnect from the resource.

In version 4.0 of LAN Server, all aliases (both local to the domain and those external to the domain) are treated as internal aliases (in fact, they must be declared INTERNAL).

Adding Aliases - Files

To create a new file alias, you will first have to create a file entry in the [ALIAS_ADD] section and then create a complete file alias reference section to match. The entry in the [ALIAS_ADD] section appears as follows:

`File = `**`NEW_ALIAS_NAME`**

Where:

`File` - the type of alias to add

`NEW_ALIAS_NAME` - the name of the alias to create

Each detail section is made up of the base name of "`[ALIAS_FILE_`" followed by the name of the new alias in the format: "`NEWALIAS]`". See the example below as an example.

Example:

```
[ALIAS_ADD]

       file = ROOT_C
       file = ROOT_D


[ALIAS_FILE_ROOT_C]
  Remark = Root directory on server
  File_Path = C:\
  Location = INTERNAL
  Server = \\DMNPL
  Mode = DYNAMIC
  Max_Uses = UNLIMITED
  Net_Name = ROOT_C

[ALIAS_FILE_ROOT_D]
  Remark = Root directory on server
  File_Path = D:\
  Location = INTERNAL
  Server = \\DMNPL
  Mode = DYNAMIC
  Max_Uses = UNLIMITED
  Net_Name = ROOT_D
```

In this example, we have created two file aliases within the domain.

Key to File Alias Detail Section Contents

Remark =	Supplied comment about the new alias. Must be no greater than 40 characters in size.
File_Path =	Path on server to be shared. This is normally a drive letter followed by a path such as D:\OS2. Path length limited to 128 characters
Location =	**INTERNAL** = Within Domain **EXTERNAL_DOS** = Outside domain & accessed by DOS workstations only **EXTERNAL_OS2** = Outside domain & accessed by OS/2 workstations only **EXTERNAL_BOTH** = Outside domain & accessed by all workstations Note: only INTERNAL may be used within LAN Server 4.0 domains
Server =	Server that holds the resource to share. Server names must be in the format of \\Server_name
Mode =	**STARTUP** = Shared when server started **BYADMIN** = Must be explicitly shared by administrator **DYNAMIC** = Resource is shared at the time of request
Max_Uses =	Maximum number of users that can share this alias at one time
Net_Name =	Same as alias name

Adding Aliases - Printers

To create a new printer alias, you will first have to create a printer entry in the [ALIAS_ADD] section and then create a complete printer alias reference section to match. The entry in the [ALIAS_ADD] section appears as follows:

Printer = **NEW_ALIAS_NAME**

Where:

Printer - the type of alias to add

NEW_ALIAS_NAME - the name of the alias to create

Each detail section is made up of the base name of "[ALIAS_PRINTER_" followed by the name of the new alias in the format: "NEWALIAS]". See the example below as an example.

```
Example:

[ALIAS_ADD]

        printer=LASER1
        printer=LASER2


[ALIAS_PRINTER_LASER1]
  Remark=Network Laser #1
  Queue_Name=LASERN1
  Location=INTERNAL
  Server=\\DMNPL
  Mode=DYNAMIC
  Max_Uses=UNLIMITED
  Net_Name=LASERN1

[ALIAS_PRINTER_LASER2]
  Remark=Network Laser #2
  Queue_Name=LASERN2
  Location=INTERNAL
  Server=\\DMNPL
  Mode=DYNAMIC
  Max_Uses=UNLIMITED
  Net_Name=LASERN2
```

In this example, we have created two file aliases within the domain.

Key to Printer Alias Detail Section Contents

`Remark`	Supplied comment about the new alias. Must be no greater than 40 characters in size.
`Net_Name`	Queue Name (ignored on alias add)
`Queue_Name`	Name of printer queue (object) on the server
`Location`	**INTERNAL**=Within Domain **EXTERNAL_DOS**=Outside domain & accessed by DOS workstations only **EXTERNAL_OS2**=Outside domain & accessed by OS/2 workstations only **EXTERNAL_BOTH**=Outside domain & accessed by all workstations Note: only INTERNAL may be used within LAN Server 4.0 domains
`Server`	Server that holds the resource to share. Server names must be in the format of \\Server_name
`Mode`	**STARTUP**=Shared when server started **BYADMIN**=Must be explicitly shared by administrator **DYNAMIC**=Resource is shared at the time of request
`Max_Uses`	Maximum number of users that can share this alias at one time
`Net_Name`	Same as alias name

Adding Aliases - Serial

To create a new serial alias, you will first have to create a serial entry in the [ALIAS_ADD] section and then create a complete serial alias reference section to match. The entry in the [ALIAS_ADD] section appears as follows:

Serial=**NEW_ALIAS_NAME**

Where:

Serial - the type of alias to add
NEW_ALIAS_NAME - the name of the alias to create

Each detail section is made up of the base name of "[ALIAS_SERIAL_" followed by the name of the new alias in the format: "NEWALIAS]". See the example below as an example.

Example:

```
[ALIAS_ADD]

      serial=MODEM1
      serial=MODEM2


[ALIAS_SERIAL_MODEM1]
  Remark=Network MODEM #1
  Queue_Name=MODEM1
  Location=INTERNAL
  Server=\\DMNPL
  Mode=DYNAMIC
  Max_Uses=UNLIMITED
  Net_Name=MODEMN1
  Priority=1
  Device_Pool=COM1

[ALIAS_SERIAL_MODEM2]
  Remark=Network MODEM #2
  Queue_Name=MODEM2
  Location=INTERNAL
  Server=\\DMNPL
  Mode=DYNAMIC
  Max_Uses=UNLIMITED
  Net_Name=MODEMN2
  Priority=1
  Device_Pool=COM1
```

In this example, we have created two file aliases within the domain.

Key to Serial Alias Detail Section Contents

Remark	Supplied comment about the new alias. Must be no greater than 40 characters in size.
Queue_Name	Identical to alias name
Location	**INTERNAL**=Within Domain **EXTERNAL_DOS**=Outside domain & accessed by DOS workstations only **EXTERNAL_OS2**=Outside domain & accessed by OS/2 workstations only **EXTERNAL_BOTH**=Outside domain & accessed by all workstations Note: only INTERNAL may be used within LAN Server 4.0 domains
Server	Server that holds the resource to share. Server names must be in the format of \\Server_name
Mode	**STARTUP**=Shared when server started **BYADMIN**=Must be explicitly shared by administrator **DYNAMIC**=Resource is shared at the time of request
Max_Uses	Maximum number of users that can share this alias at one time
Net_Name	Queue name for serial port

Chapter 6 - Batch Editor: Applications

At the time of logon, LAN Server can provide the user with a folder of applications. There are two types of applications known as *private* and *public*. Public applications are potentially available to all users on the LAN (if assigned as parts of the user add or update process). Private applications are set-up for each user and allow each user to have a series of unique applications.

The LAN Intensive Care Utilities supports the who range of public and private application capabilities including multiple alias to drive assignments at application startup (like the NET USE command).

Before assigning a public application to a user, it must first be created. This is accomplished by listing the name of the application in a [APP_ADD] section. If the user wishes to have private applications, these are created by creating a detailed section with the name: [APP_PRIVATE_userid_appname]. This naming convention assures that each user can have unique private applications.

There are two operation sections for applications: [APP_ADD] and [APP_DELETE].

IMPORTANT NOTES:

If you receive the error: "Bad parameter" when creating an application, please check the following:
1) A comment must be supplied for all applications
2) All comments must be unique (you cannot have the same comment on two public applications).
3) Check that the alias and server actually exist on your domain.

Hint! If you are not certain of the format to create a public or private application, try creating one using the full-screen interface or GUI of LAN Server. Then, use the "LU -APP" to see the application definitions. If you are creating a private application, then use the command: "LU - USERS" to see how things were formatted.

Deleting Public Applications

To delete public applications, you will have to create entries in a [APP_DELETE] section. The entries in the [APP_DELETE] section appears as follows:

Os2App = APPLICATION_NAME
DosApp = APPLICATION_NAME

where:

Os2App = OS/2 application type
DosApp = DOS application type
APPLICATION_NAME = Name of application to delete

Example:

[APP_DELETE]

        Os2App=PMEYES
        DosApp=WORDSTAR

In this example, we will delete the OS/2 application called PMEYES, and the DOS application known as WordStar.

Adding Public Applications

To create a new public application, you will first have to create an appropriate public application entry in the [APP_ADD] section and then create a complete public application reference section to match. The entry in the [APP_ADD] section appears as follows:

```
Os2App = APPLICATION_NAME
DosApp = APPLICATION_NAME
```

where:

```
Os2App =  OS/2 application type
DosApp =  DOS application type
APPLICATION_NAME =  Name of the application to
```
delete

Example:

```
[APP_ADD]

        Os2App=PMEYES
        DosApp=WORDSTAR

[APP_PUBLIC_PMEYES]
  App_Name=PMEYES
  App_Remark=Desktop utility to follow cursor
  App_Command=PMEYES
  App_Command_Parms=<NONE>
  App_Alias_or_Drv=ROOT_C
  App_Path_to_Dir=\UTILS
  App_Wrkdir_Alias_or_Drv=<NONE>
  App_Wrkdir_Path_to_Dir=<NONE>
  App_Wrkdir_Drive=LOCAL
  App_Prompt=NO
  App_Interface=PROT
  App_Type=OS2_PUBLIC

[APP_PUBLIC_WORDSTAR]
  App_Name=WORDSTAR
  App_Remark=DOS Word Processing Package
  App_Command=WS
  App_Command_Parms=<NONE>
  App_Alias_or_Drv=ROOT_C
  App_Path_to_Dir=\WS
  App_Wrkdir_Alias_or_Drv=<NONE>
  App_Wrkdir_Path_to_Dir=<NONE>
  App_Wrkdir_Drive=LOCAL
  App_Prompt=YES
  App_Interface=
  App_Type=DOS_PUBLIC
```

In this example, we will delete the OS/2 application called PMEYES, and the DOS application known as WordStar.

75

Key to Public application Detail Section Contents

`APP_Remark`	Supplied comment about the application. Must be no greater than 40 characters in size.
`APP_Command`	Command to start the program
`App_Command_Parms`	Command line parameters to supply at program start
`App_Alias_or_Drv`	Alias or drive letter where the application resides. If the application resides on the local machine, use a drive letter (C:) or an alias if the application resides on the server.

`App_Path_to_Dir`	Remaining path information to get to application program. This must begin with "\".
`App_Wrkdir_alias_or_Drv`	Working directory for application to run from. Can be an alias or a local drive letter depending on where the application is running. No entry means that no working directory is supplied. This is like a CD NEWPATH
`App_Wrkdir_Drive`	Working drive letter to application to run from. This is like logging onto a drive before running an application. For OS/2 apps this can be from "D" to "Z". For DOS apps, this can be from "A" to "X". A value of "*" signifies that the LAN should pick the next free drive letter. If the application is running locally, there should be no entry in this field.
`App_Wrkdir_Path_to_Dir`	Remaining path information to get to application program. This must begin with "\". If `App_Wrkdir_Alias_or_Drv` is blank, this should also be left blank.
`App_Prompt`	Command prompt requested at program start. `YES` - Request command line arguments before starting app `NO` - No request for command line arguments
`App_Interface`	`PM` - Presentation Manager application `PROT` - Non-windowed protect mode application `VIO` - Non-PM application that uses OS/2 video I/O `(blank)` - DOS applications
`App_Type`	`DOS_PUBLIC` - Public DOS Application `OS2_PUBLIC` - Public OS/2 Application `OS2_PRIVATE` - Private OS/2 Application

App_Asn	Drive Assignments when program operating.
	
	This line allows you make LAN alias assignments to local drive letters on the user's workstation. If an asterisk '*' is entered instead of a drive letter, the first available free drive will be used instead. This command is equivalent to a NET USE command performed at logon.
	
	The syntax is as follows:
	`Logon_Asn=`
	`TYPE:LOCAL PERIPHERAL:ALIAS`
	
	Where:
	`TYPE=FILE,PRINTER,` or **`SERIAL`**
	`LOCAL PERIPHERAL=`
	  `FILE:  A:..Z:, or *`
	  `SERIAL: COM1:..COM9`
	  `PRINTER: LPT1:..LPT9`
	
	  `ALIAS=Defined domain alias`
	
	You can have multiple "`App_Asn=`" assignment lines. You cannot use physical peripheral names of devices that actually exist on your machine.

The exporter will sometimes generate a value of <NONE>. <NONE> is equivalent to no entry in the application fields where you find it. When entering values, just leave the value to right of the equal sign blank.

Chapter 7 - Batch Editor: Groups

Groups are handled in a two part process. First, the Batch Editor will look for sections marked as [GROUP_ADD], [GROUP_DELETE], and [GROUP_UPDATE]. The [GROUP_ADD] section allows you to create a group name and set its comment. The [GROUP_DELETE] removes the group from the domain. The [GROUP_UPDATE] allows you to change the comment on an existing group. These group management sections are processed at the beginning of Batch Editor's operation, so that users may successfully add themselves to a group that already exists. If the user attempt to add themselves to a group that does not exist, an error will be generated.

The second task performed for groups is the management of their member lists. For controlling the member list, we have the [GROUP_USER_ADD] and [GROUP_USER_DELETE] section lists. The basic operations are to add and delete users from groups. These sections are processed at the very end of the Batch Editor's operation. This operation must be done last, since we cannot add users to a group that do not exist (the user add operation is performed before the group user management).

As in all the other parts of the Batch Editor, you supply a list of sections to process and the editor takes care of the rest. In this case, the detail sections referred to are the same as the [GROUP_name] sections produced by the exporter (LU.EXE). Group detail sections contain the comment of the group as well as a list of "member=userid" entries. The detail group sections are handled twice. First, only the comment is used from the detail section when adding, deleting, or updating the group itself. When members are added or deleted, the member list for the named group is used.

Deleting Groups

To delete groups, you will have to create entries in a [GROUP_DELETE] section. The entries in the [GROUP_DELETE] section appears as follows:

GROUP = GROUP_NAME

where:

GROUP = Signifies a group operation
GROUP_NAME = Name of the group to delete

You do not have to supply a detail section for groups that you are deleting.

Example:

[GROUP_DELETE]

        GROUP=TECH1
        GROUP=WORD1

In this example, we will delete the TECH1 and WORD1 groups.

NOTE! Do not attempt to modify the groups known as: USERS, ADMINS, LOCAL, or GUESTS. These are reserved group names. Also, be careful when making changes to the group known as SERVERS as this is used for interdomain administration.

Adding Groups

To create a new group, you will first have to create the appropriate group entry in the [GROUP_ADD] section and then create a complete group detail reference section to match. The entries in the [GROUP_ADD] section appears as follows:

GROUP = GROUP_NAME

where:

GROUP = Signifies a group operation
GROUP_NAME = Name of the group to add

You do not have to supply a group detail section for the [GROUP_ADD] operation. A default comment will be supplied if there is no detail section. You must first create a group before you can add members to it.

NOTE! Do not attempt to modify the groups known as: USERS, ADMINS, LOCAL, or GUESTS. These are reserved group names. Also, be careful when making changes to the group known as SERVERS as this is used for interdomain administration.

Example:

```
[GROUP_ADD]

     GROUP=TECH1
     GROUP=WORD1


[GROUP_TECH1]
    Comment=Technicial Support group 1
    Member=MOE
    Member=LARRY
    Member=SHEMP

[GROUP_WORD1]
    Comment=Word Processing Team 1
    Member=JACKN
    Member=BEAN
    Member=STALK
```

In this example, we add the groups know as GROUP_TECH1 and GROUP_WORD1. Please note that the users are NOT added during the group add operation. The user add must be done with a different section known as [GROUP_USER_ADD] that is processed at the end of the batch.

Updating Groups

All you can update in a group is its comment. To update the
comment, you will first have to create the appropriate group entry in
the [GROUP_UPDATE] section and then create a group detail
reference section with a new comment. The entries in the
[GROUP_UPDATE] section appears as follows:

GROUP = GROUP_NAME

where:

GROUP = Signifies a group operation
GROUP_NAME = Name of the group to update

NOTE! Do not attempt to modify the groups known as: USERS,
ADMINS, LOCAL, or GUESTS. These are reserved group names.
Also, be careful when making changes to the group known as
SERVERS as this is used for interdomain administration.

Example:

```
[GROUP_UPDATE]

        GROUP=TECH1
        GROUP=WORD1


[GROUP_TECH1]
      Comment=NEW Technical Support group 1
      Member=MOE
      Member=LARRY
      Member=SHEMP

[GROUP_WORD1]
      Comment=NEW Word Processing Team 1
      Member=JACKN
      Member=BEAN
      Member=STALK
```

In this example, we will update the groups know as GROUP_TECH1 and
GROUP_WORD1 with new comments. Please note that the users are NOT
updated during the group update operation. The user add or delete must be done
with different sections known as [GROUP_USER_ADD] and
[GROUP_USER_DELETE] that are processed at the end of the batch.

Deleting Users in Groups

To delete users in groups, you will have to create entries in a [GROUP_USER_DELETE] section. The entries in the [GROUP_USER_DELETE] section appears as follows:

GROUP = GROUP_NAME

where:

```
GROUP =  Signifies a group operation
GROUP_NAME =  Name of the detail group section containing
              list of members to delete
```

You MUST supply a detail section for all users with a group that you are deleting.

Tips!

1) In the detail group section you are not forced to use the format "Member=Userid." You can also use "User=Userid" or "Admin=Userid" or "User_template=Userid." This allows you to cut and paste entries directly from the [USER_LIST] section.

2) In most cases you will get the detail group lists directly from the output of the exporter utility (LU.EXE) so that a minimum of typing is really needed (just some cut and paste).

Example:

```
[GROUP_USER_DELETE]

      GROUP=TECH1
      GROUP=WORD1


[GROUP_TECH1]
      Comment=Technicial Support group 1
      Member=SHEMP

[GROUP_WORD1]
      Comment=Word Processing Team 1
      Member=STALK
```

In this example, we will delete Shemp as a member of the TECH1 group, and Stalk as a member of the WORD1 group.

NOTE! Do not attempt to modify the members of groups known as: USERS, ADMINS, LOCAL, or GUESTS. These are reserved group names. Also, be careful when making changes to the group known as SERVERS as this is used for interdomain administration.

Adding Users to Groups

To add users in groups, you will have to create entries in a [GROUP_USER_ADD] section. The entries in the [GROUP_USER_ADD] section appears as follows:

GROUP = GROUP_NAME

where:

 GROUP = Signifies a group operation
 GROUP_NAME = Name of the detail group section containing
                 list of members to add

You MUST supply a detail section for all users with a group that you are adding.

Tips!

1) In the detail group section you are not forced to use the format "Member=Userid." You can also use "User=Userid" or "Admin=Userid" or "User_template=Userid." This allows you to cut and paste entries directly from the [USER_LIST] section.

2) In most cases you will get the detail group lists directly from the output of the exporter utility (LU.EXE) so that a minimum of typing is really needed (just some cut and paste).

Example:
```
[GROUP_USER_ADD]

     GROUP=TECH1
     GROUP=WORD1


[GROUP_TECH1]
     Comment=Technicial Support group 1
     Member=CURLY
     Member=JOE

[GROUP_WORD1]
     Comment=Word Processing Team 1
     Member=STALK

```

In this example, we will delete Shemp as a member of the TECH1 group, and Stalk as a member of the WORD1 group.

NOTE! Do not attempt to modify the members of groups known as: USERS, ADMINS, LOCAL, or GUESTS. These are reserved group names. Also, be careful when making changes to the group known as SERVERS as this is used for interdomain administration.

Key to Group Detail Section Contents

`APP_Remark`	Supplied comment about the application. Must be no greater than 40 characters in size.
`APP_Command`	Command to start the program
`App_Command_Parms`	Command line parameters to supply at program start
`App_Alias_or_Drv`	Alias or drive letter where the application resides. If the application resides on the local machine, use a drive letter (C:) or an alias if the application resides on the server.
`App_Path_to_Dir`	Remaining path information to get to application program. This must begin with "\".
`App_Wrkdir_alias_or_Drv`	Working directory for application to run from. Can be an alias or a local drive letter depending on where the application is running. No entry means that no working directory is supplied. This is like a CD NEWPATH
`App_Wrkdir_Drive`	Working drive letter to application to run from. This is like logging onto a drive before running an application. For OS/2 apps this can be from "D" to "Z". For DOS apps, this can be from "A" to "X". A value of "*" signifies that the LAN should pick the next free drive letter. If the application is running locally, there should be no entry in this field.

`App_Wrkdir_Path_to_Dir`	Remaining path information to get to application program. This must begin with "\". If `App_Wrkdir_Alias_or_Drv` is blank, this should also be left blank.
`App_Prompt`	Command prompt requested at program start. `YES` - Request command line arguments before starting app `NO` - No request for command line arguments
`App_Interface`	`PM` - Presentation Manager application `PROT` - Non-windowed protect mode application `VIO` - Non-PM application that uses OS/2 video I/O (`blank`) - DOS applications

App_Type	DOS_PUBLIC - Public DOS Application OS2_PUBLIC - Public OS/2 Application OS2_PRIVATE - Private OS/2 Application

App_Asn	Drive Assignments when program operating.
	
	This line allows you make LAN alias assignments to local drive letters on the user's workstation. If an asterisk '*' is entered instead of a drive letter, the first available free drive will be used instead. This command is equivalent to a NET USE command performed at logon.
	
	The syntax is as follows:
	`Logon_Asn=`
	`TYPE:LOCAL PERIPHERAL:ALIAS`
	
	Where:
	`TYPE=FILE,PRINTER,` or `SERIAL`
	`LOCAL PERIPHERAL=`
	`  FILE:  A:..Z:, or *`
	`  SERIAL: COM1:..COM9`
	`  PRINTER: LPT1:..LPT9`
	
	`  ALIAS=Defined domain alias`
	
	You can have multiple "`App_Asn=`" assignment lines. You cannot use physical peripheral names of devices that actually exist on your machine.

Chapter 8 - Batch Editor: Access Control Lists

Overview

Access controls allow the system administrator to control access to resources on the server. The implementation of the system is pretty simple. First, permissions can be granted to both users and groups. You can have up to 64 permission entries (called Access Control Entries (ACEs)) per resource. This restriction of 64 permissions per resource is removed when using HPFS-386.

Resources that have permissions include serial ports, printer queues, disks, directories, and files. The most common level of permission is the directory for disk devices. The following picture illustrates the relationship between resources and permissions.

Resource Name   **Access Control List**

C:\MAGNUM

+

Audit Conditions

USER:MOE Permissions:RWX
USER:LARRY Permissions:R
GROUP:USERS Permissions:X
GROUP:ACCT Permissions:W

Up to 64 ACE's per resource

Access Control Entries
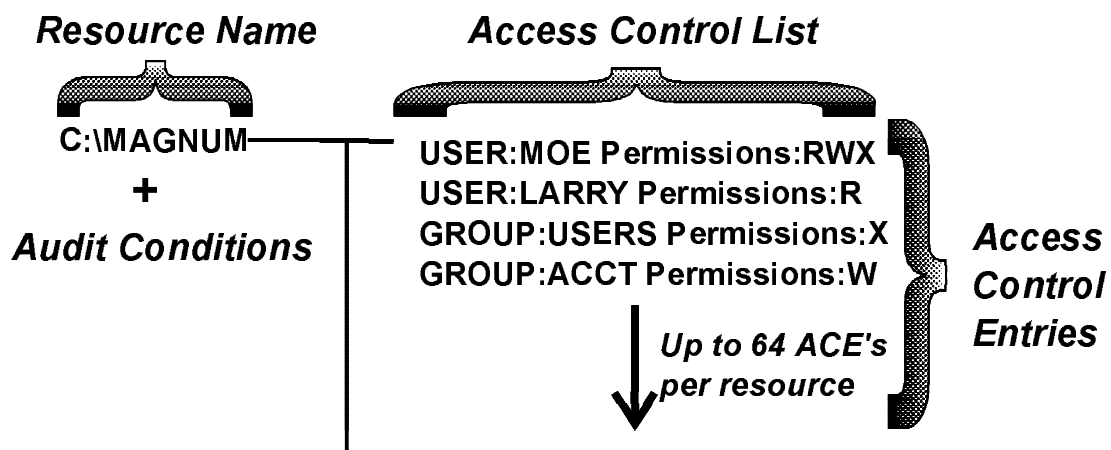
The exporter utility provides this information in two forms. First sorted by server, drive, and resource name. This first report is the access control list report. The second report sorts the information given in the first report by user and group. The second report shows the access control entries (ACEs) for each user and group. The second report shows what each user and group have permissions. This is important when auditing a system to determine level of access. Without this report, you would have to look at every resource and check for a specific user's name (pretty much impossible except on the simplest system). The following picture illustrates the two reports generated by the exporter.

Exporter (LU.EXE)

ACCESS Report

ACLs

Access Control Lists by Server

ACEs

Access Control Lists by Users & Groups
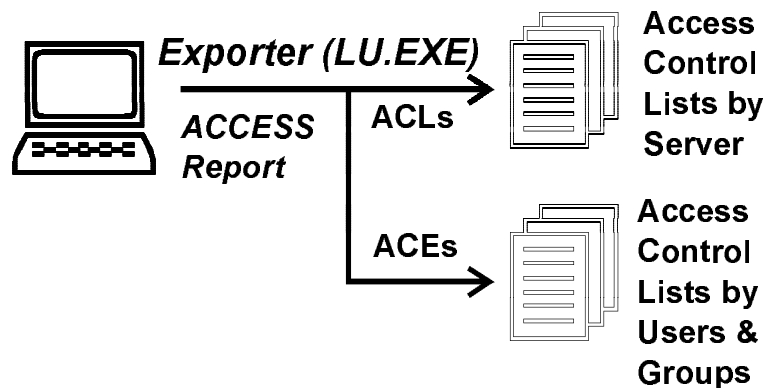
Moving Information

You can move access control information using two methods: by resource (ACL method) or by user/group (ACE method). In this section we will explore both types of information and how it is migrated.

You would use the resource method of moving access control information when you are moving entire subdirectories from machine to machine. By using this method, all user, group, and audit information is moved as a group--the complete set of permissions on a resource (subdirectory) is known as the Access Control List. Typically this method is used when upgrading hard disks, adding new servers, or moving aliases from place to place.

When all we wish to move is a user or group from place to place, but we wish to keep the resource in place, we can use the ACE method of permission migration. For every resource in LAN Server (also known as a file directory) there is a list of access control entries (known as ACEs). Each ACE entry identifies the users and groups that have permissions to access that resource.

Access Control List Movement (by resource)

The Batch Editor can now Add, Delete, Update, and Move access control lists from server to server. You no longer have to move user or group information.

In the ACE sections you have to specify the names of the users and/or groups that are to be moved. With this feature, you can move all of the ACEs associated with a specific resource or group of resources in one shot. This is handy when you want to move users from one server to another.

In the [ACCESS_ADD], [ACCESS_DELETE], and [ACCESS_UPDATE] sections you have the following entries:

SERVER=ServerName

> Name of the **[ACCESS_SERVER_ServerName]** section containing the ACL entries to be used.

Adding Resources

The following example will add two access control lists to the following resources on the server called \\SRVPHIL:

- C:\MAGNUM\WORK_DIR\1
- C:\MAGNUM\WORK_DIR\2

Example:

```
[ACCESS_ADD]
 Server=SRVPHIL

[ACCESS_SERVER_SRVPHIL]
 ACL=C:\MAGNUM\WORK_DIR\1  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R

 ACL=C:\MAGNUM\WORK_DIR\2  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R
```

Deleting Resources

This example will delete all of the access control lists contained in the section entitled: [ACCESS_SERVER_SRVPHIL]

```
Example:

[ACCESS_DELETE]
 Server=SRVPHIL

[ACCESS_SERVER_SRVPHIL]
 ACL=C:\MAGNUM\WORK_DIR\1  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R

 ACL=C:\MAGNUM\WORK_DIR\2  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R
```

Updating Resources

```
Example:

[ACCESS_UPDATE]
 Server=SRVPHIL

[ACCESS_SERVER_SRVPHIL]
 ACL=C:\MAGNUM\WORK_DIR\1  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R

 ACL=C:\MAGNUM\WORK_DIR\2  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R
```

This example will update all of the access control lists contained in the section entitled: [ACCESS_SERVER_SRVPHIL]

Moving Resources

One problem in moving resources from place to place is the need to edit the source files so that the server name matches the target server getting the new resources. In this latest version, you can retain the name of the original server section, and target one or more different servers with the same access control lists. This is a handy feature when you want to duplicate access on multiple machines.

This is accomplished by the **SERVER_MOVE** command that is used in the **[ACCESS_ADD]** and **[ACCESS_DELETE]** sections.

   SERVER_MOVE=From_Server,To_Server

```
Example:

[ACCESS_ADD]
 Server_Move=SRVPHIL,BACKSRV1
 Server_Move=SRVPHIL,BACKSRV2
 Server_Move=SRVPHIL,BACKSRV3
 Server_Move=SRVPHIL,BACKSRV4

[ACCESS_SERVER_SRVPHIL]
 ACL=C:\MAGNUM\WORK_DIR\1  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R

 ACL=C:\MAGNUM\WORK_DIR\2  ;\\SRVPHIL
  GROUP=G1 Perm=ALL
  GROUP=USERS Perm=X
  GROUP=LOCAL Perm=W
  GROUP=GUESTS Perm=R
```

This example will copy all of the access control lists contained in the section entitled: **[ACCESS_SERVER_SRVPHIL]** to the servers: **BACKSRV1, BACKSRV2, BACKSRV3, BACKSRV4**. You must have already copied all of the files in these subdirectories to the targets before copying the permissions.

Resource Migration Tips and Techniques

These new features in **BA.EXE** and **LU.EXE** were designed to make the migration of users from server to server as painless as possible. To accomplish the move, use the batch editor to extract all of the ACLs based on the subdirectory that the user or users are working with. Next, copy the files and subdirectories to the new machine using an identical subdirectory structure.

Finally, add an **[ACCESS_ADD]** section to the original ACL capture and insert the line:

```
Server_Move=OriginalServer,NewServer
```

Run the batch editor using the just modified ACL capture, and the newly moved files will have all of their ACLs in place.

Note: You must have added the user and group accounts to the new target machine(s) before moving the access control lists.

Deleting ACEs

To delete access control entries for a user or group you would first create a section called: [ACCESS_DELETE]. Next you would add the user or group name of a detail section containing the details of that user's ACEs. Below is an example:

```
Example:
[ACCESS_DELETE]
 user=a1
 group=g1

[USER_ACL_A1]
  ACE=\\SRVPHIL C:\IBMLAN\DCDB\USERS\A1 Perm=ALL
  ACE=\\SRVPHIL C:\IBMLAN\DCDB\USERS\A1\BATCH Perm=ALL
  ACE=\\SRVPHIL D:\Z8 Perm=ALL
  ACE=\\SRVPHIL D:\Z8\BIN Perm=ALL
  ACE=\\SRVPHIL D:\Z8\C8 Perm=ALL
  ACE=\\SRVPHIL D:\Z8\HELP Perm=ALL
  ACE=\\SRVPHIL D:\Z8\INCLUDE Perm=ALL

[GROUP_ACL_G1]
  ACE=\\SRVPHIL C:\51 Perm=ALL
  ACE=\\SRVPHIL C:\51\AM Perm=ALL
  ACE=\\SRVPHIL C:\51\DMI Perm=ALL
  ACE=\\SRVPHIL C:\AM Perm=ALL
  ACE=\\SRVPHIL C:\BELKIN Perm=ALL
  ACE=\\SRVPHIL C:\BETAS Perm=ALL
```

In the above example we are removing the listed access control entries for the user known as "A1" and the group known as "G1".

Adding ACEs

To add access control entries for a user or group you would first create a section called: [ACCESS_ADD]. Next you would add the user or group name of a detail section containing the details of that user's ACEs. Below is an example:

Example:
```
[ACCESS_ADD]
 user=a1
 group=g1

[USER_ACL_A1]
  ACE=\\SRVPHIL C:\IBMLAN\DCDB\USERS\A1 Perm=ALL
  ACE=\\SRVPHIL C:\IBMLAN\DCDB\USERS\A1\BATCH Perm=ALL
  ACE=\\SRVPHIL D:\Z8 Perm=ALL
  ACE=\\SRVPHIL D:\Z8\BIN Perm=ALL
  ACE=\\SRVPHIL D:\Z8\C8 Perm=ALL
  ACE=\\SRVPHIL D:\Z8\HELP Perm=ALL
  ACE=\\SRVPHIL D:\Z8\INCLUDE Perm=ALL

[GROUP_ACL_G1]
  ACE=\\SRVPHIL C:\51 Perm=ALL
  ACE=\\SRVPHIL C:\51\AM Perm=ALL
  ACE=\\SRVPHIL C:\51\DMI Perm=ALL
  ACE=\\SRVPHIL C:\AM Perm=ALL
  ACE=\\SRVPHIL C:\BELKIN Perm=ALL
  ACE=\\SRVPHIL C:\BETAS Perm=ALL
```

In the above example we are adding the listed access control entries for the user known as "A1" and the group known as "G1".

Updating ACE Permissions

To update access control entries for a user or group you would first create a section called: [ACCESS_UPDATE]. Next you would add the user or group name of a detail section containing the details of that user's ACEs. Below is an example:

Example:

```
[ACCESS_UPDATE]
 user=a1
 group=g1

[USER_ACL_A1]
  ACE=\\SRVPHIL C:\IBMLAN\DCDB\USERS\A1 Perm=ALL
  ACE=\\SRVPHIL C:\IBMLAN\DCDB\USERS\A1\BATCH Perm=ALL
  ACE=\\SRVPHIL D:\Z8 Perm=ALL
  ACE=\\SRVPHIL D:\Z8\BIN Perm=ALL
  ACE=\\SRVPHIL D:\Z8\C8 Perm=ALL
  ACE=\\SRVPHIL D:\Z8\HELP Perm=ALL
  ACE=\\SRVPHIL D:\Z8\INCLUDE Perm=ALL

[GROUP_ACL_G1]
  ACE=\\SRVPHIL C:\51 Perm=ALL
  ACE=\\SRVPHIL C:\51\AM Perm=ALL
  ACE=\\SRVPHIL C:\51\DMI Perm=ALL
  ACE=\\SRVPHIL C:\AM Perm=ALL
  ACE=\\SRVPHIL C:\BELKIN Perm=ALL
  ACE=\\SRVPHIL C:\BETAS Perm=ALL
```

In the above example we are updating the listed access control entries for the user known as "A1" and the group known as "G1".

Moving Access Control Permissions

To change the location of a resource such as an alias, first capture all of the ACEs for that alias using the LU.EXE utility (`LU -ACCESS -O:MOVEACC.ICU`). Next, find group permissions for the ACEs that apply to the alias to be moved. Modify the server name and/or drive location for the ACEs that are going to be moved so they reflect the new location of the ACEs. Finally, create an [ACCESS_ADD] section and put in the name of the group containing the new ACE list. Run the batch editor with the command:

> `BA -I:MOVEACC.ICU -O:LOG.DAT`

That should do the trick. You may also want to move the ALIAS definitions also. Information on doing this is in this manual.

Chapter 9 - The Analyzer: How it Works
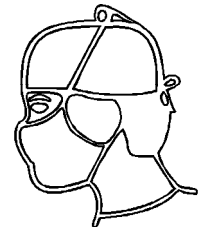
Background on Analyzer

The problem faced by many domain administrators is the impossibility of verifying every user's account and the resources associated with the user. Consequently, most administrators just do their best, cross their fingers, and hope things will not break. This is not a good situation.

When we set out to design a domain analyzer we envisioned a tool that would use some form of artificial intelligence to dissect your domain and check for common and uncommon errors--and correct them. The analyzer does what you would do if you had the time and patience to really go through hundreds of users methodically.

Rules

The key to the analyzer is the rules file. This is just a modified export ASCII file similar to the file used for the batch editor. In this file you will be creating sections with different [RULE_...] section names. The following 'rules' sections will be found in a typical rules file:

User Privilege Rule **+** Operator Privileges Rule(s) **+** Group Membership Rule(s) *Yields* User's Rule-Based Profile **?** **=** Actual User's Profile

✂ **Delete Extra Entries**

✓ **Add Missing Entries**

Based on differences perform actions needed
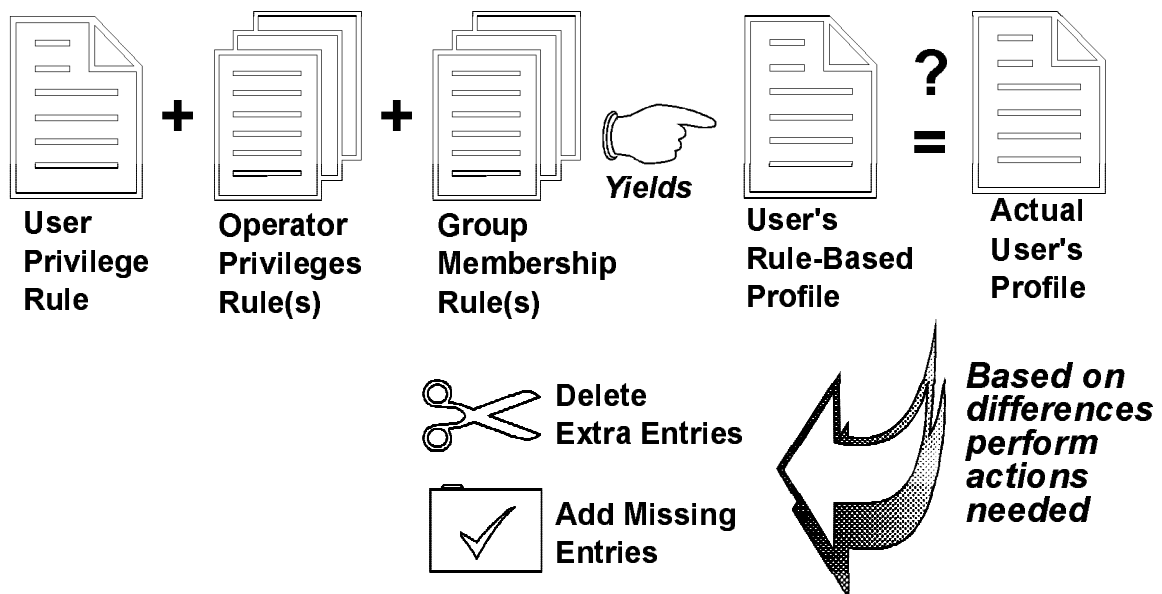
Privilege Rules	
[RULE_USER]	Base user account for accounts with USER authority
[RULE_ADMIN]	Base user account for accounts with ADMINISTRATOR authority
[RULE_GUEST]	Base user account for accounts with GUEST authority
Operator Rules	
[RULE_OPER_COMM]	Rules for communication operator privilege
[RULE_OPER_SERVER]	Rules for server operator privilege
[RULE_OPER_PRINT]	Rules for print operator privilege
[RULE_OPER_ACCOUNTS]	Rules for accounts operator privilege
[RULE_ORDER]	List of groups from highest to lowest priority
[RULE_GROUP_name]	Added settings for members of group '_name'

Fill in the information in the rules section using the same format as all other sections.

The rules are broken down into three groups:

1) Privilege based rules - initial account settings to use based on account privilege.

2) Operator based rules Operator based rules - operator rules are applied after the user privilege
2) Group based rules - additional rules based on an account group memberships.

To figure out what is right and wrong with a user account, we must first build a reference account for comparison. To do this, a series of rule sections will be read in to build the reference account.

How each reference account is built for the analyzer

To build a user reference account, the analyzer will first look at the user privilege and then load the appropriate [RULE_priv] section into the reference account. Next it will look through the group memberships and add all of the [RULE_GROUP_name] sections (those they exist) to the reference account. When all of the available group sections have been added, the user account will be compared to the reference account built from the rule sections. Any discrepancies will be pointed out and you will be given the chance to change each user setting that is different to the value in the just built reference account.

Each rule section may contain a series of base parameters as well as logon parameters. The base parameters used within each section are summarized in the following table:

- Account_Active
- Account_Deletable
- Password_Required
- Password_Changable
- Password_Age
- Privilege
- Logon_Script
- Script_Path
- Home_Dir_Required
- Home_Dir

- Operator
- Application_Parms
- Workstations
- Account_Expires
- Max_Storage
- Logon_Hours
- Logon_Server
- Country_Code
- Code_Page

Logon assignments are also part of each group's profile. These are the logon assignment supported:

- **Logon_Asn**   Alias logon assignments

- **AppSel**   Public application logon assignments

Privilege rules

Why did we do thing this way? We needed some way to build a reference account to check each user. We decided that the common base characteristic of all accounts is their privilege. This became the base rule to which all other rules are added.

If you were to run the analyzer with only the privilege rules, you would quickly find that even in the simplest system, there are differences between users. For example, servers also have user accounts, yet their settings are completely different from normal user accounts. When the analyzer hits a server user account, it immediately flags it as an account with inconsistent settings. Of course, in a normal production system, users belong to different groups, and different groups have different logon assignments.

To improve the ability of the analyzer to deal with these varying situations, we also have *group rules*.

Group Rules

A group rule is nothing more than another user section that only contains the settings and assignments that are different for a member of that group. Typically, groups only contain alias and program logon assignments. However, as we discussed earlier, you will want to also change base settings for users such as 'servers'.

To create a rule section for a group, we use the format [RULE_GROUP_name]. For example, to create a set of settings for our servers, we would simply create a section called: [RULE_GROUP_SERVERS].

Users that belong to multiple groups

If a user belongs to multiple groups, all of the sections from all of the different groups will be combined together and then compared to the user's account settings. Any discrepancies will be pointed out and the analyzer will offer to fix any differences.

There is a fly in the ointment though. What would happen if a user was a member in multiple groups, yet some groups require user settings one way, yet other groups require the exact opposite setting. In this case, the analyzer will use the rule that was applied last if it makes the last change. But, which rule is applied last?

A good example of this problem is our friend the server again. The server belongs to the groups: USERS and SERVERS. Because the groups are normally executed in alphabetically order, USERS will be the last and final word on how the server should be set-up (U comes after S)--this will most likely create the wrong effect. So how do we ensure that our group rules are applied in the proper order? The answer is a special section called [RULE_ORDER].

Rule Order - forcing the processing order of group rule sections

The [RULE_ORDER] is a section of the format:

    GROUP=SERVERS
    GROUP=FIRE
    GROUP=LIFE
    GROUP=AUTO
    GROUP=MARINE
    GROUP=USERS

The list above is prepared from most important rule to least important rule. Also, the first entries in the [RULE_ORDER] are really applied last to an account. This "first is really last" rule makes sense because the most important rules are the last ones to be applied since they override any previous settings. Note: Logon assignments are always added (alias and program); base settings are always overridden (i.e. Password_Required) by new settings in a group rule.

The reference account is assembled by starting with a base memory image, followed by the appropriate privilege account rule. The last step is to get all the user's group memberships, sort them according to the order listed in the [RULE_ORDER] and then apply each group's rule section until all of the sections has been processed. Once all of the sections have been applied to the reference account, it is then compared with the user's account.

If you do not prepare a [RULE_GROUP] section, then groups will be applied in alphabetical order (probably not what you want).

Preparing a rule set for your domain

To make your life easier, we have provided a default RULE.ICU file to show you what a default rule file would look like. By the way, if you forget to explicitly call out the name of the rules file for the analyzer, the file RULES.ICU will be used as a default.

As a first step, you should probably add rule sections for the groups in your domain. In each of these groups, add the logon assignments for members of that group. You can have duplicate assignments in different groups. The analyzer will alert you to the duplications, but will process the accounts correctly.

On the following page you can see the default rules file.

```
;   Example rules file: RULES.ICU
;
;
;   Part 1 are the base settings based on
;   privilege only.
;
;
[RULE_USER]
  Account_Active=YES
  Account_Deletable=YES
  Password_Required=YES
  Password_Changable=YES
  Password_Age=44 Days 23:06:21
  Privilege=USER
  Logon_Script=YES
  Script_Path=
  Home_Dir_Required=NO
  Home_Dir=
  Operator=
  Application_Parms=
  Workstations=
  Account_Expires=NEVER
  Max_Storage=UNLIMITED
  Logon_Hours=ALL
  Logon_Server=\\*
  Country_Code=0
  Code_Page=437
  Member_of=USERS

[RULE_ADMIN]
  Account_Active=YES
  Account_Deletable=YES
  Password_Required=YES
  Password_Changable=YES
  Password_Age=44 Days 23:06:21
  Privilege=ADMIN
  Logon_Script=YES
  Script_Path=
  Home_Dir_Required=NO
  Home_Dir=
  Operator=
  Application_Parms=
  Workstations=
  Account_Expires=NEVER
  Max_Storage=UNLIMITED
  Logon_Hours=ALL
  Logon_Server=\\*
  Country_Code=0
  Code_Page=437
  Member_of=ADMINS


[RULE_GUEST]
  Account_Active=YES
  Account_Deletable=YES
```

```
  Password_Required=NO
  Password_Changable=YES
  Password_Age=58 Days 22:37:52
  Privilege=GUEST
  Logon_Script=YES
  Script_Path=
  Home_Dir_Required=NO
  Home_Dir=
  Operator=
  Application_Parms=
  Workstations=
  Account_Expires=NEVER
  Max_Storage=UNLIMITED
  Logon_Hours=ALL
  Logon_Server=\\*
  Country_Code=0
  Code_Page=437
  Member_of=GUESTS
;
;   Part II contains the group rules
;
;   Priority of group processing.  Top of
list
;   is processed last.
;
[RULE_ORDER]
  GROUP=SERVERS
  GROUP=FIRE
  GROUP=LIFE
  GROUP=CAR
  GROUP=USERS
;
;  Typical profile of server
;
[RULE_GROUP_SERVERS]
  Account_Active=NO
  Account_Deletable=YES
  Password_Required=NO
  Password_Changable=YES
  Password_Age=58 Days 22:37:53
  Privilege=USER
  Logon_Script=YES
  Script_Path=
  Home_Dir_Required=NO
  Home_Dir=
  Operator=
  Application_Parms=
  Workstations=
  Account_Expires=NEVER
  Max_Storage=UNLIMITED
  Logon_Hours=ALL
```

```
Logon_Server=                        Member_of=SERVERS
Country_Code=0                       Member_of=USERS
Code_Page=437
```

How analyze tells you what rules it uses

The first line of the report for each user shows you the privilege followed by the userid of the user to be analyzed. At the end of the first line you will also see the user comment (i.e. 'Admin = Phil1 ;This is Phil's account').

On the next line you will see the entry "Rule base:" that shows you the order of rules used to process this userid for proper operation (i.e. 'PRIV_ADMIN >ADMINS(?) >') . The first entry in the line is the privilege rule(i.e. PRIV_ADMIN >). The arrow shows the direction of processing. If the next entry does not have a group section describing what to do for that group, a question mark in inserted after the name (i.e. ADMINS(?) >). By looking across the line of rules being used, you can see how the analyzer determined what the "correct" profile is for the user.

The analyzer recalculates the profile for each user based on their unique privilege and group memberships. You should not worry that some groups do not have rules, as their effect may be inconsequential in determining the final outcome of the rule analysis.

System duplication of privilege and group rules

Every account with USER level privilege will automatically be a member of the 'USERS' group. For ADMIN level accounts, they are all members of the 'ADMINS' group. Finally, all members with GUEST level privilege will be a member of the group 'GUESTS'. As a result of this default relationship, there is no need to define a group rule for and of the groups: USERS, ADMINS, or GUESTS. A possible use of this default membership might be to force some settings at the end of processing by making these groups the highest priority.

Messages you will see while running the analyzer

The message "`Extra Application`" means that according to the group membership assignments (GROUP RULES) and user privilege assignment (PRIV RULES) for this user, the application listed is not correct. In English, the program looked at all of the groups the user belongs to, and the user's privilege, and based on all of the rules you provided, the application listed should not be assigned to this user.

Solution: Add this user to an additional group(s) that should get this application as part of its rules. Or, if you do not want to deal with this exceptional case, just ignore the message.

The message: "`Extra Logon Alias`" is exactly the same thing as "`Extra Application`" except in this case it could not find an "`Logon_Asn`" in any group rule that matches what the user has assigned. The solution again is to add the user to a group that has this logon alias assignment as part of its rule base.

You may also see the message "`Missing Application`" and "`Missing Logon Alias`". In these cases the user belongs to a group that should have the listed assignments, but the user is missing them. When the utility is run, you have the option of adding the missing assignments by just pressing the "Y" key.

Running the Analyzer

There are a few general rules regarding the use of command line options used in the LU.EXE program. First, the normal setting for the program is to act as though the options for ALIAS, USERS, XREF, MODALS, BANNER, GROUPS, ACCESS are all enabled. If you select one or more of the foregoing options, the rest are turned off. This method of selecting single or multiple options is designed to make reporting as flexible as possible.

The order of parameters on the line is not important. Generally, only the first three letters of a report are needed. For example, you can select the alias option with "-ALI", or you can select users with the option "-USE". Of course, if the parameter requires a file name, the whole parameter must be typed in.

```
AN.EXE 951228 - Syntax:  AN [switches] [-O:LOGFILE]
 Analyze from the 'LAN Intensive Care Utilities' for
     IBM LAN Server
  Copyright 1994,1995,1996 - Lieberman and Associates
     Design and Engineering Group

 -[O:LOGFILE_NAME] (To send analysis to file)
 -[I:RULE_FILE_NAME] (Rule definitions - Default
File:RULES.ICU')
 -[F:FIX_FILE_NAME] Fix file for batch editing -
     Default:'FIXLAN.ICU'
 -[UN:StartUserId],EndUserId-limits actions to single/range
     of userids
 -[B]atch - send all changes to FIX file (for BA.EXE)
 -[Y]es   Answer YES to all questions
 -[N]o    Answer NO  to all questions
 -[XBA]SE   Skip testing base user settings based on rules
 -[XLO]GON  Skip testing logon assignments(apps/aliases) based
     on rules
 -[XDC]DB    Skip testing integrity of DCDB for user
 -[XPE]RMISSIONS  Skip testing permissions for user alias
      assignments
 -[DOM:DOMAIN_NAME] (override logon domain name)
 -[SRV:SERVER_NAME] (override primary domain controller name)
 -[Q]uiet flag - turns off output to console only
 -[V]erbose flag - provides detail operating status during
     operations

 Default settings are all analysis enabled and console output.
 Selecting any one analysis, disables the rest unless they are
 also selected on the command line.  You may put the
parameters
 in any order you wish.  Capitalization is not important.
```

-[Q]uiet – turns off output to console only

> Normally the output of the LU.EXE program goes to the display. If
> you are capturing the output of the program using the "-O" option,
> you may not want to see the identical output scroll on the screen.
> This option turns off the program's output to the screen.

-[O:LOGFILE NAME] (To send report to file (append mode)
-[AO:LOGFILE NAME] (To send report to file (append mode)

> This option allows you to capture the output of the program into a file.
> Note that the log file operates in an "append" mode; adding the
> output of each run to the end of the last. If there is no existing file of
> the name given in this parameter, the program will create it.

-[RO:LOGFILE NAME] (To send report to file (replace mode)
-[WO:LOGFILE NAME] (To send report to file (replace mode)

> Operates like the previous "-O" option except it replaces the previous
> log file with a new one for the current run. You may want to use this
> option if you are using the LAN ICU package with REXX scripts
> where the logs are archived. The "RO" and "WO" options do the
> same thing.

-[F:FIX FILE NAME] (Specifies fix file name usable by BA.EXE))

> The batch file flag must be on (-B) for the fix file to be used. If there is no fix file name given, the default name of "FIXLAN.ICU" will be used.

-[B]atch mode (Operates Analyzer in batch mode)

> Starting with version 1.3, you can now run the Analyzer program in detached mode (no-user interaction required). The program can then generate a fix file that can be used directly by the BA.EXE program. The batch file flag must be on for the fix file to be used. If there is no fix file name given, the default name of "FIXLAN.ICU" will be used.

-[UN:StartUserID],EndUserId -limits reports to a range of userids)

> You can limit operations in the analyzer to only a selected group of users with the command line switch of:

> > -unStartId,EndID

> This option can be used a number of ways to limit the scope of your operations with these utilities. With this option you can select a single user or a range of users depending on where they are in the alphabetical list.

> ### Selecting a single user

> To select a single user, just enter the userid of the user as the sole parameter (no commas). For example, to just export the account called ACURLY using the rule file called RULE.ICU, enter the following command:

> > AN -i:RULE.ICU -un:ACURLY

> ### Selecting a range of users

> With this option you can limit the operations to a range of alphabetic characters. The first parameter specifies the starting name and the second parameter specifies the ending name. If neither name is the name of an actual user, their alphabetic value will be used.

> For example, to analyze all of the user accounts start are in the range from "A" to "G" (last account is account G - account name GOPHER would not be included since it is greater than G), you would enter the following command:

> > AN -i:RULE.ICU -un:A,G

> You can also write this as all of the accounts up to and including the letter G with the command:

> > AN -i:RULE.ICU -un:,G

> You can also specify all of the accounts after a name or letter by just specifying the first argument with a comma. For example, to specify all of the account that occur after and including USERID, you would use the following command:

> > AN -i:RULE.ICU -un:USERID,

– **[XBA]SE**

Skips testing of base profile settings like password required, logon server, etc.

– **[XLO]GON**

Skips testing of alias and application logon assignments.

– **[XDC]B**

Skips testing of DCDB integrity and initialization. If you have users with uninitialized DCDBs, and you do not want them flagged, use this option.

– **[XPE]RMISSIONS**

Skips testing access permissions for accounts. This feature will not check the user's right to use the aliases that are assigned at logon.

– **[BAN]NER Report**

The banner information shows you the revision of the software. Also shown are the user and company name. Use this option to quickly check the version of software you are using.

– **[DOM:DOMAIN_NAME] (override logon domain name)**

This parameter provides the administrator with cross domain administration capabilities. Without this parameter the utility will operate only on the domain that the administrator has logged into. With this parameter, you can operate on a domain other than the one logged into.

For this feature to work, the userid and password must be identical between the logged-in domain, and the one specified in this argument.

– **[SRV:SERVER_NAME] (override primary domain controller name)**

Normally the utilities within the LAN ICU package will use the server defined as the primary domain controller within the domain. This argument allows you to target another server within the domain. Possible targets include backup domain controllers.

Forcing answers in the analyzer

You have a command line option to force the answer of "yes" or "no" for all questions in the analyzer. You would use this option if you wished to just see what the current state of a domain was without making any changes or corrections to it. When you have reviewed the changes, you would then set the switch to "YES". To limit the changes to only a selected range, you might use the previously described "-un" or user name option switch to specify the range inclusive of the start and stop names.

The option switch is simple. To answer "NO" to all questions, just use the switch of "-N".   To answer "YES" to all questions, just use the switch of "-Y" on the command line.

For example, to get an analyze report of the accounts from JONES to SMITH without any changes, issue the following command:

```
AN -i:RULE.ICU -un:JONES,SMITH -N
```

By the way capitalization is not important in the switches. Order of the parameters on the line is also not important. What is important though, is that you may not add any spaces after the colon character (:) or dash character (-) unless you are entering another switch setting.

Chapter 10 - Problems fixed by the ANALYZER

Uninitialized DCDB

If you create an account but never assign it
application or alias logon assignments, network errors
will occur every time the user logs on, or when their
account is referenced. This problem is known as the
Uninitialized DCDB problem. We see it as a LAN
error code 3, also known as a network file not found
error. When the analyzer detects this situation, we
offer to correct it by initializing the user's DCDB area.
This step creates an empty, yet correct DCDB files.
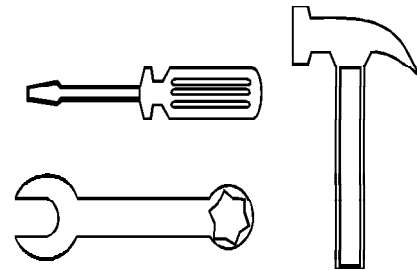
In some case where you have migrated from LAN Server 2.0 to 3.0 you may bring
forward half initialized DCDB files. We also detect this and create the missing half
automatically.

Non-existent ALIAS

If you have ever seen the dreaded "Some of your logon aliases have failed" you will
appreciate this feature. After all of the rules have been applied, the analyzer will
check for the existence of aliases on the network. If you have reconfigured your
network by adding and deleting aliases, you may still have users with logon
references to non-existent aliases.

This problem is picked up in the exporter by the XREF or cross reference report.
When the analyzer is run, it will also test for the existence of aliases in the
composite rule as well as the user's account. You will have the option of deleting
references to obsolete aliases.

WARNING: If you have a server that has gone off-line, the aliases that were on that
server will disappear. The most common cause of the error: "some of your
assignments have failed" is an off-line server__. Do not have the analyzer delete
references to aliases on off-line servers.__

Please run the exporter with the -SERVER option to confirm that all of the known
servers are up an running before removing references to so-called non-existent
aliases.

Lack of sufficient privilege

This is a biggie! After all of the rules have been applied and before moving on to
the next account, the analyzer will verify that all logon aliases are really available to
the user. This is accomplished by checking the if the user has sufficient privilege
based on the user's group memberships and user privileges. If there is no privilege,
you will get a warning message: "*** No Permissions" on the alias assignment.

WARNING: The analyzer will not stop on accounts that have insufficient privilege
since correcting this problem requires decisions regarding group and user
permissions that are at the sole discretion of the administrator. It is a good idea to

use the log file feature to keep a record of all errors and changes. After running analyze program, examine the log file for any user accounts with permission problems. This is a common problem!

Duplicate application & alias entries

A bug in earlier versions of LAN Server allowed the administrator to add the same application twice (or more) to the user account. In the full screen interface you would only see the single application no matter how many times you added it. Internally LAN Server kept each redundant copy. As a result, you would find that you were unable to delete applications. The analyzer checks for these redundant entries and corrects the corruption for you.

You must have the supplied LRSD.DLL file installed on your domain controller for ANALYZE to correct this problem. You should also have installed the IP7045 Service Pack.

Deleted but not removed application entries

Damage can sometimes appear in the DCDB where public applications are removed, but internally LAN Server did not clean up properly. We detect and correct this internal problem also.

You must have the supplied LRSD.DLL file installed on your domain controller for ANALYZE to correct this problem. You should also have installed the IP7045 Service Pack.

Chapter 11 - Domain Definition Report Converter Domain Definition Report Converter

Converter (CV.EXE) - Domain Definition Report Converter

If you are currently running LAN Server 1.0 or 2.0 and want to migrate to a newer version of LAN Server, this utility help performs the conversion. The utility takes the "Domain Definition Report" from the LAN Requester and converts it into the format used by the batch editor (BA.EXE).
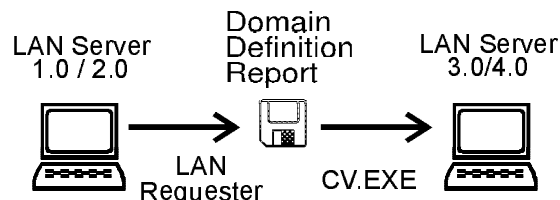
To get a "Domain Definition Report" from the LAN Requester, set the Printer Status setting of the printer into the "HOLD" state. Send the Domain Definition Report to the jets "held" printer queue. Next, open the printer object and double-click on the just captured output file. Last, save the file under a name and subdirectory that is convenient for you. You may want to delete the print job from the printer queue and change the printer state to "Released".

Once you have the capture report, you can then convert it into the format used by the batch editor with the CV.EXE program.

The format of the CV.EXE command is:

```
CV -I:Input_File -O:Output_File -W:Working_directory
```

The domain definition report does not specify a working directory for user accounts, only a drive letter. The "-W:" parameter allows you specifies the remaining part (after the existing drive letter) of the working directory for the user account. Because each user will want their own subdirectory, you can add the "%U" parameter anywhere in the working directory parameter. The userid name will be substituted when the "%U" parameter is encountered.

For example, if you had the domain definition report called: PHIL.LAN and wanted to create the file: PHIL.ICU with a working directory of \ACCT\USERNAME, you would use the following command:

```
CV -I:PHIL.LAN -O:PHIL.ICU -W:\ACCT\%U
```

Chapter 12 - Patches & Problems
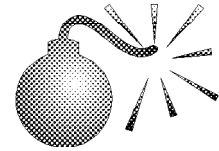
Warp Server

We have tested the operation of LAN ICU on Warp Server and everything seems to be functioning fine. As this is a new product from IBM, keep your checking for patches as they become available. We will post information on our BBS regarding any problems and workarounds.

Warp Connect - Peer Services

If you attempt to run LAN ICU using peer services rather than with LAN Requester, you may get an error indicating that administrative privilege is required to use the software. This error is caused by the lack of an administrative account for your current logon within one of the machines in the peer group. The solution is to add your administrator account to the peer machine, or to temporarily stop the peer services on the machine that is appearing in your domain.

The solution to this error is to use the LAN Requester software within Warp Connect to administer the domain that your are working on.

LAN Server 4.0

In the initial releases of the LAN Server 4.0 package, we encountered numerous bugs that would cause traps to occur at random times when running the LAN ICU package. These traps seem to occur more frequently when running from a server or the domain controller. Corrective Service Diskettes (CSDs) from IBM correct these problems.

If you do not have, or do not want to apply the CSDs, another temporary solution to these problems is to run from a requester. With the patches applied to LAN Server 4.0, you should have very few (if any) problems using LAN ICU on your domain.

IP7060

You will have all kinds of problems using this service pack on LAN Server 3.0. We recommend bypassing this service pack on requesters. If you ignore our advice, you will encounter an error that indicates that you have lost administrative privilege when using the LAN ICU package.

If you are using IP7060 you will get an error code 5 or 65 from LAN ICU. Here is a work around that seems to work OK. Before using the LU or AN programs, make sure that you are logged on as an administrator and enter the following commands:

```
NET USE \\SERVER1\IPC$ <ENTER>
NET USE \\SERVER2\IPC$ <ENTER>
NET USE \\SERVER3\IPC$ <ENTER>
```

where SERVER1, SERVER2, SERVER3 would be the names of all YOUR servers in the domain.

The purpose of these lines is to force your requester to make a validated connection for the purposes of intermachine communications. This NET USE step is not supposed to be needed, but due to a bug in LAN Server, failure to do so may cause some of your data to not be exported due to the misimpression that you are not an administrator (at least to some servers, and only sometimes).

Once the NET USE operations have been performed, they stay in effect until you logoff.

IP7045

We have heard many stories about this patch from no problems to nightmares. We have been using it in our shop with no difficulties. We also have it in other shops with no problems. For proper operation of the LAN ICU package you must have the service pack applied. If you have not applied the service pack, you may see garbage in the data field of aliases when running the exporter. You should also not run the analyzer on domains without this service pack as you may see gibberish in the alias entries. If you do run the utility without the service pack, you may have errors with aliases. Many of the fixes in IP7045 are a result of problems we reported to IBM during the development of the LAN ICU package.

LRSD.DLL

If you are using public or private applications, you must install the supplied LRSD.DLL file to your domain controller. This replacement library allows us to delete defective application entries as well as build external aliases properly. The consequence of not having this newer library installed is a report of a "6273" undocumented error when retrieving some user accounts. You may also see garbage in the public and private application areas of a user's account when running the export utility.

The LRSD file supplied with your software, or from our BBS is newer than the IP7045 service pack. You should apply the service pack first, then replace the LRSD file. If you replace it and then run the service pack installation, the service pack will replace our newer file with the older one on the service pack (and all of the problems will reappear).

Chapter 13 - Revision History of LAN ICU
Revision History of LAN ICU

New Features of version 1.4 (rev 951228)

General Improvements 12/28/95

This version rolls in all of the improvements over the last few months. These improvements include better performance, patches, and new features.

Added the ability to operate the log files in both append or replace mode. The original "-O" option still operates in append mode. The new "-RO" option operates in "replace" mode (also known as write (vs append) mode). Finally an end to those growing log files.

Image size of BA.EXE, AN.EXE, and LU.EXE was significantly reduced by combining the common error message files into a single module within ICULIB.DLL. You will need to use this new DLL with these new modules. Watch those LIBPATHS!

Improved BA.EXE 12/28/95

Completed improvements of the home directory creation process. All operations to the user's home directory are now recorded.

ACE update code was revised to assure that resource names could not be corrupted diring the addition of new ACEs. The corruption problem would not cause any damage to the domain, the error exhibited itself as the inability to add ACEs to a resource.

Improved AN.EXE - 11/22/95

Made single image AN.EXE and LU.EXE.

Improved LU.EXE - 11/21/95

Added catch code for ACLs returned as wildcards (error 2222)

LU now uses 32-bit code when running on LS40 or above requester (single image version) .

Fixed trap in -RSRC that could occur in LUNEW release

Speeded up the ACL output (went back to single step NetAccessInfo method)

Correction to 11/05/95 Release - 11/16/95

A small bug in the new -RSRC code caused regular resource names to be interpreted as aliases in all cases. This has been corrected in this release. Now both resource names and alias names are recognized properly.

New LAN Intensive Care Utilities for IBM LAN Server - 11/05/95 Version 1.3D

This LU.EXE version breaks through the 64K barrier for the -RSRC command. For you convenience, you can also supply only the ALIAS name as the resource argument (the other arguments are optional if you are using an alias name).

-RSRC alias options

With this version you can now retrieve the ACLS based on an alias name. For example, to extract the ACLS for the alias "ROOT_D", you would enter the following command:

```
LU -RSRC:,ROOT_D
```

When using the alias option, you do not need the server name, as this information is picked up from the alias definition.

-RSRC 64K limit lifted

This version now handles the case of more than 64K worth of data available for a resource path.

-RSRC Server Header Information Added

In previous versions, you needed to create a [Server_List] section. This version automatically adds this header information.

Release: Version 1.3C - 8/13/95

This version keeps track of your domains and serial numbers. If you are running in a multiple domain environment and do not have a site license (this feature is turned off for site licenses), you will need to install a different serial numbered version for each domain.

Consequently, you will need to run the registration If you have a registered copy of LAN ICU and it will not exit from demo mode after registration, please contact Lieberman and Associates.

Ability to run from any requester

The registration process (REG.EXE) now copies the unlock key to the domain controller so that programs can now be put on the server and run from any requester without having to copy the LAN ICU software to that requester.

NOTE: This version now uses DLL files. Consequently, you will need to set the 'working directory' to the same location as the LAN ICU executable files and DLL files.

Multiple LU ACL runs possible

You can now run multiple copies of LU while extracting access control lists. In the previous versions a common temporary file was created that would only allow one LU.EXE program to run at a time. Attempting to run multiple copies would cause a trap. This version implements temporary files so you can run as many copies of LU.EXE as you wish.


```
-F option (Filter)
```

Filtering ACLs for only files/directories etc.

One of the most requested features for ACLs was the ability to filter the output of the ACL report to just files or directories. This has been accomplished with a new command line switch in the LU.EXE program. The '-F:' or filter switch takes any single or combination of letters as follows to control the filtering of ACLs:

```
F - Files
D - Directories
N - Non-existent directories (seen on FAT only)
P - Printers
C - Communications (Serial ports)
I - Pipes
O - Others (anything other than the above)
```

For example, to just list the files with ACLs on a domain, enter:

```
LU -ACL -F:F
```

To list the printers, communciation ports, and pipes, enter the following:

```
LU -ACL -F:PCI
```

The filter will also affect the ACE reporting; only showing those users that have ACEs that meet the filter criteria.

If you do not supply a filter parameter, the default of ALL is assumed.

```
-[ISRV:SERVER_NAME,SERVER_NAME...]
      Operate only on these servers

-[XSRV:SERVER_NAME,SERVER_NAME...]
      Exclude these servers
```

Include/Exclude Servers

When accumulating information from a large domain, the amount of data can become enormous. To minimize the data, we have provided two commands: one to exclude certain servers (to exclude problematic servers), and another to specify the servers to export. Depending on your needs, you could use either of these commands.

Home Directories

This version automatically creates home directories when using the batch editor (BA.EXE) to create or update user accounts.

Each home directories receives full permission for the user assigned to it.

ACL Enumeration Correction - 7/13/95

LU.EXE now properly exports the ACL/ACE permission of "A" (permission to modify attributes) on the resource (it was skipped in previous implementations). Note: if

you had the "ALL" permission, all of the bits were set; it was just in individual combinations this was not exported.

Workarounds & Product improvement for IP7060 Service Pack - 7/5/95

The traps experienced with running with the IP7060 service pack should now be a thing of the past. This also goes for some problems you might have experienced with LAN Server 4.0. Most of these traps were caused by LAN Server returning bad data at different times. The code now has tests for these circumstances.

2) If you get an error code 5 or 65, here is a work around that seems to work OK. Before using the LU program, make sure that you are logged on as an administrator and enter the following commands:

```
NET USE \\SERVER1\IPC$ <ENTER>
NET USE \\SERVER2\IPC$ <ENTER>
NET USE \\SERVER3\IPC$ <ENTER>
```

where `SERVER1, SERVER2, SERVER3` would be the names of all YOUR servers in the domain.

The purpose of these lines is to force your requester to make a validated connection for the purposes of intermachine communications. This NET USE step is not supposed to be needed, but due to a bug in LAN Server, failure to do so may cause some of your data to not be exported due to the misimpression that you are not an administrator (at least to some servers, and only sometimes).

Once the NET USE operations have been performed, they stay in effect until you logoff.

3) The APP_DRIVE parameter is now displayed for both DOS and OS/2 public/private applications. According to the LAN Server 3.0 documentation, this field is not used by OS/2 applications. After trying the LS40 GUI, it is apparent that this can be set for all applications now.

ABOUT THIS NETUSERMODAL PROBLEM

IBM has identified the cause of the Error 5 and 65 and they are working on a fix for both LAN Server 3.0 and 4.0. This has been fixed in all service packs beyond IP7060.

New Features of version 1.3 (rev 950103)

New Features LU Exporter (rev 950103)

Faster Operation

Improved performance of single/range of user export. This version now skips all users that are not needed. This improves performance radically.

Real-Time Status Display

New "-V" option provides Verbose status information about all operations. This gives you a progress report of all operations (especially when handling >64K of

ACLs). A graphical display shows you the speed of different operations. We normally add this option to all of our command lines so that we can gauge when an operation will be completed. The verbose status information does not go into the log files since it provides you with visual cues only.

Detect and Repair Access Control Lists

New "-BAD" option checks access control entries for access lists. Empty ACLs and non-existent directories/files with resources are flagged. The program now generates a file: FIXACL.ICU that can used in the BA program to erase the bad entries. Each entry is annotated.

Possible Trap Condition Corrected

Corrected bugs that could cause a trap if a drive was checked for ACLs and there were none.

Added Selection Criteria for Groups and ACEs

-UN: Option now limits user and group information for USER, GROUP, and ACEs This allows you to export the access control information for a single user/group.

ACE or ACL Only Reports Now Available

Export data for access control can be limited to either -ACL (resources/server) or -ACE (users/groups/server) information. Both are listed by -ACC (all access information). Using the -UN option you can now export the access control info for a specific user or group.

Import DCDB & NET.ACC Info Without Editing

In this version you can change the header sections from [..._LIST] to ADD, UPDATE, or DELETE sections using the new -E option. The next letter after -E stands for the type of section(s) to generate. A=ADD, D=DELETE, U=UPDATE. This is then followed by a colon followed by the type of resource section to change. The resource names are: [USE]ER, [GRO]UP, [ALI]IAS,[APP]LICATIONS,[ACL],[ACE],[ALL]. You can use more than one option at a time. The ALL option changes all sections that are generated.

For example, to change the user export from a list to an ADD, you would enter the command:

```
-EA:USER
```

To change the ACE entries from LIST to UPDATE, you would use the command:

```
-EU:ACE
```

For example, to refresh the access permissions for the user "PHIL" with the file REFRESH.ICU you would use the following command to create the change file:

```
LU -ACE -UN:PHIL -EU:ACE -V -O:REFRESH.ICU
```

To then apply this newly created file, you would use the command:

```
BA -I:REFRESH.ICU
```

Servers and Users Now Listed in ACL and ACE sections

We now provide lists of servers, users, and groups that are in access sections. The lists can be renamed to [ACCESS_ADD], [ACCESS_DELETE], and

[ACCESS_UPDATE] using the -E option. This allows access sections to be processed in BA.EXE with no editing needed. Lists of users/groups can be narrowed with -UN option.

Adjustable Buffer Size for Large ACLs

When accessing directory entries from remote servers that have large drives, you can control the buffering of entries. You can buffer 1, 3 or 64K worth of directory entries. When accessing a LAN Server 3.0 domain with HPFS-386 from an LAN Server 4.0 requester, only the 1 entry buffer should be used (bug in LAN Server 4.0)--this is the default. In other cases you can use the larger buffer size. The option is controlled with the switches:

```
-BUF1     Buffer one directory entry only (default)
-BUF3         Buffer 3 entries
-BUF64K   Buffer a full 64Kbytes of entries (best
performance)
```

Cross Reference Report Now Shows Logon Assignments

Added functionality to cross reference report. This version not displays the logon assignment for each user in the report. If you want to make sure that all of the users have the same logon assignments, this feature shows you all of your logon assignments by resource.

Command Line, Userid, and Machine ID now echoed

Additional information is now provided on all reports.

Rewrote Exporter to handle LAN Server Internal Error

In some cases, LAN Server would return an error code of 2140 (LAN Server Internal Error). This version uses a rewritten version to work around this LAN Server bug. We also achieved faster user info lookup also.

Exported Encrypted Passwords Might not be Importable

This version now truncates the password to 32 characters in both the importer and exporter. This will allow you to use existing files with control characters in the Encrypted Password field.

New Features in BA.EXE Batch Editor Module (Version: 941229)

Add to Group USERS & ADMINS Now Ignored

If an attempt was made to add a user to the USERS group, a LAN error would occur. Now attempts to add a user to both USERS and ADMINS are ignored.

DOS DCDBs Now Synchronized

Any changes to Alias or Application logon assignments now cause the DOS DCDB files to be synchronized automatically. The DOS DCDB can be manually synchronized to the OS/2 DCDB.

A bug exists in both LAN Server 3.0 and 4.0 that can cause the DOS DCDB files to not be synchronized with the OS/2 database. This causes logon assignments to

work properly for OS/2 workstations, but not for DOS workstations. DOS workstations users find extra assignments as well as many missing assignments.

The "`Sync_DOS_DCDB=YES`" option forces the DOS DCDB files to be synchronized with the OS/2 DCDB files. The following sequence can be used to synchronize a series of users manually using the template 'FIXDOS':

```
[USER_UPDATE]
  User_FIXDOS=PL
  User_FIXDOS=SRVICS
  User_FIXDOS=SRVPHIL
  User_FIXDOS=TESTC
  User_FIXDOS=TESTD
  User_FIXDOS=TESTE
  User_FIXDOS=TESTF
  User_FIXDOS=TESTG
  User_FIXDOS=U01
  User_FIXDOS=USERIX
  User_FIXDOS=X1
  User_FIXDOS=X10
  User_FIXDOS=X2

[USER_FIXDOS]
Sync_DOS_DCDB=YES
```

This file would be used as input to the Batch Editor.

New Options in Fix File

'`Init_DCDB=YES`' option is used to clear a user's logon DCDB. This option will be added to the fix file of any user that has an uninitialized DCDB.

'`Fix_App_DCDB=YES`' option is inserted if an internal consistency error is detected in a user's DCDB.

User name can be changed without editing

A new option has been added to allow an existing exported user section to be reimported under a new name without editing the export file. This feature is accomplished with the '-CN:OldName,NewName' option. The change name feature operates on user add, delete, and update operations.

This feature is designed to allow a single user to be changed. If there are muliple user names in the export file, only the user section that matches the OldName will be used for the NewName.

Memory buffer too small on some application adds

In some cases applications might not be added due to a limited buffer size. This has been corrected.

Encrypted Password Imports might fail

In some versions of LAN Server, the encrypted password might contain an embedded control character at the end of the password. This situation is now detected and only the first 32 characters are used. This allows existing exported user sections to be used with no problems.

Import DCDB & NET.ACC Info Without Editing

In this version you can change the header sections from [..._LIST] to ADD, UPDATE, or DELETE sections using the new -E option. The next letter after -E stands for the type of section(s) to generate. A=ADD, D=DELETE, U=UPDATE. This is then followed by a colon followed by the type of resource section to change. The resource names are: [USE]ER, [GRO]UP, [ALI]IAS,[APP]LICATIONS,[ACL],[ACE],[ALL].You can use more than one option at a time. The ALL option changes all sections that are generated.

For example, to import a user section from a LIST to an ADD, you would enter the command:

> **-EA:USER**

To change the ACE & ACL entries from LIST to UPDATE, you would use the command:

> **-EU:ACL**

For example, to refresh the access permissions for the user "PHIL" with the file REFRESH.ICU you would use the following command to create the change file:

> **LU -ACE -UN:PHIL -V -O:REFRESH.ICU**

To then apply this newly created file, you would use the command:

> **BA -I:REFRESH.ICU -EU:ACL**

New Features in AN.EXE Analyzer Module (Version: 941229)

DOS DCDBs Now Synchronized

A bug exists in both LAN Server 3.0 and 4.0 that can cause the DOS DCDB files to not be synchronized with the OS/2 database. This causes logon assignments to work properly for OS/2 workstations, but not for DOS workstations. DOS workstations users find extra assignments as well as many missing assignments.

This has been rectified via a number of solutions. First, when checking user accounts, the synchronization of DOS and OS/2 logon files is checked. If there is an inconsistency, then the user is offered the opportunity to perform a **DOS_DCDB_SYNC** operation (YES/NO). There are two files dealt with during the sync operation: LIST.S (application assignments) and LIST.U (alias assignments). Both are synchronized to the OS/2 DCDB.

If the batch option is chosen, the Analyzer will now insert the line: "Sync_DOS_DCDB=YES" into the batch file to force the Batch Editor to do the synchronization. This line can be added manually to a change section to cause a series of users to be synchronized. For example, the following sequence can be used for synchronization a series of users manually using the template 'FIXDOS':

```
[USER_UPDATE]
  User_FIXDOS=PL
  User_FIXDOS=SRVICS
  User_FIXDOS=SRVPHIL
  User_FIXDOS=TESTC
  User_FIXDOS=TESTD
  User_FIXDOS=TESTE
  User_FIXDOS=TESTF
  User_FIXDOS=TESTG
```

```
User_FIXDOS=U01
User_FIXDOS=USERIX
User_FIXDOS=X1
User_FIXDOS=X10
User_FIXDOS=X2
```

```
[USER_FIXDOS]
Sync_DOS_DCDB=YES
```

This file would be used as input to the Batch Editor.

Analyzer Now Creates Batch Files

One of the most requested features in LAN ICU was the ability to use the Analyzer in batch mode to create a change file that could be examined and run at a later date. This feature has now been implemented in both the Analyzer and Batch Editor.

The switch to perform the analyze operation in batch mode is '-B'. This causes all problems and their solutions to be inserted into a fix file that can be used for input to the Batch Editor. The name of the batch file is controlled by the: '-F:FIXFILENAME' parameter. If no fix file name is supplied, the default file name of FIXLAN.ICU will be used.

Analyzer Can Be Limited in Scope

Another feature widely requested was the ability to turn off the rules base or selected parts of it. This can now be accomplished by the following command line switches:

`[-XBA]SE`   Skips testing of base profile settings like password required, logon server, etc.

`[-XLO]GON`   Skips testing of alias and application logon assignments.

`[-XDC]B`   Skips testing of DCDB intergity and initialization. If you have users with uninitialized DCDBs, and you don't want them flagged, use this option.

`[-XPE]RMISSIONS`   Skips testing access permissions for accounts. This feature will not check the user's right to use the aliases that are assigned at logon.

Faster Operation of Analyzer

The user name [-UN] option has been speeded up radically. This version will now skip forward directly to the first user account listed. It will end its operation at end of the last user.

Permissions Problems Listed in Fix File

All corrections are placed in the fix file. Insufficient privilege is flagged in fix file and must be corrected manually.

New Options in Fix File

`'Init_DCDB=YES'` option is used to clear a user's logon DCDB. This option will be added to the fix file of any user that has an uninitialized DCDB.

`'Fix_App_DCDB=YES'` option is inserted if an internal consistency error is detected in a user's DCDB.

Alias not found in domain

This version of the analyzer now checks the aliases within the domain more completely. The Alias not found in domain message now accurately reports existence or non-existence of aliases.

New Features of version 1.2 (rev 941016)

Exporter (LU.EXE) - Password Feature

This version now features the ability to export passwords in encrypted form. The exported encrypted passwords can be imported by the import utility BA.EXE. To provide the most flexibility, the passwords can be moved using any workstation or by performing the action at the domain controller itself. The export and import operations are much faster if performed at the domain controller.

To export passwords from LU.EXE you have two options:

1) Normal password export with user data. This feature adds the encrypted password with the normal user data. To enable this feature, add the "-PAS" (password) parameter. For example:

        LU -PAS -USER

This extracts all fo the user information including the passwords.

2) Sometimes you do not want all of the user data, just the passwords for the user or users. This limitation is accomplished with the "-XPA" (exclusive password). For example, to extract only the passwords use the command:

        LU -XPA -USER

Importer (BA.EXE) - Password Feature

This new version recognizes a new line in the input file:

        PASSWORD_ENCRYPTED=010203040506070809010111213141516

If this line is encountered while processing the file, the password on this account will be changed to the encrypted equivalent on the PASSWORD_ENCRYPTED line. For this feature to work, the PWDEXP.EXE and PWDIMP.EXE files must be in the working directory.

Converter (CV.EXE) - Domain Definition Report Converter

If you are currently running LAN Server 1.0 or 2.0 and want to migrate to a newer version of LAN Server, this utility helps performs the conversion. The utility takes the "Domain Definition Report" from the LAN Requester and converts it into the format used by the batch editor (BA.EXE).

Exporter (LU.EXE)

A new parameter has been added to allow you to selectively extract only a part of the access control list of a server. This feature is designed to speed the migration of access control information from one server to another.

Audit information is also extracted with each resource.

The resource parameter format is:

`LU -RSRC:SERVER,RESOURCE,RECURSIVE`

Where:

> **SERVER** = Name of server such as XYZ, ABC

> **RESOURCE** = The name of the subdirectory starting path for the resource(s) to be extracted.

> **RECURSIVE**=(Y/N) indicates whether to extract all subdirectories below the starting point given in RESOURCE. If you are extracting user subdirectories, then you want this set to "Y"es.

Important Note: The format of information on server access control lists has been changed. You will need to recapture ACL information using the new exporter (LU.EXE) to use it in the importer (BA.EXE)

Batch Editor/Importer

The Batch Editor can now Add, Delete, Update, and Move access control lists from server to server. You no longer have to move user or group information.

In the ACE sections you had to specify the names of the users and/or groups that were to be moved. With this new feature, you can do all of the ACEs associated with a specific resource or group of resources in one shot. This is handy when you want to move users from one server to another.

In the [ACCESS_ADD], [ACCESS_DELETE], and [ACCESS_UPDATE] sections you now have the following entries:

SERVER=ServerName

> Name of the [ACCESS_SERVER_ServerName] section containing the ACL entries to be used.

ANALYZER (AN.EXE)

One of the features requested in the analyzer was the inclusion of additional rules for operators. This feature has now been added as operator rules.

New Features of version 1.01 (rev 940830))

Selecting the range of UserIDs to process in analyze and exporter

In this version we have introduced the ability to limit operations in the exporter and analyzer to only a selected group of users with the new command line switch of:

```
-unStartId,EndID
```

This option can be used a number of ways to limit the scope of your operations with these utilities. With this option you can select a single user or a range of users depending on where they are in the alphabetical list.

Forcing answers in the analyzer

In this version you now have a command line option to force the answer of "yes" or "no" for all questions in the analyzer. You would use this option if you wished to just see what the current state of a domain was without making any changes or corrections to it. When you have reviewed the changes, you would then set the switch to "YES". To limit the changes to only a selected range, you might use the previously described "-un" or user name option switch to specify the range inclusive of the start and stop names.

The option switch is simple. To answer "NO" to all questions, just use the switch of "-N". To answer "YES" to all questions, just use the switch of "-Y" on the command line.

For example, to get an analyze report of the accounts from JONES to SMITH without any changes, issue the following command:

```
AN -i:RULE.ICU -un:JONES,SMITH -N
```

By the way capitalization is not important in the switches. Order of the parameters on the line is also not important. What is important though, is that you may not add any spaces after the colon character (:) or dash character (-) unless you are entering another switch setting.

Cross Domain Administration

This version allows you to export, import, and analyze any domain you wish without having to logoff and logon. All of the modules now have the - [DOM:DOMAIN_NAME] switch to allow you to enter whatever domain name you wish. You can also override the default domain controller server name using the - [SRV:SERVER_NAME] switch. You must be logged into some domain for this to work. You must also have accounts in all domains with the same userid and password with administrator authority for this to work.

Fixes in version 1.01 of LAN ICU

In the first production release the [UPDATE_USER] feature ignored all changes to the logon assignments if a standard "user=userid" entry was used. The template version of this operation did work correctly.

When processing input file in the importer and analyzer, the last line of the file was sometimes ignored if there were no blank lines at the end of the file.

The documentation incorrectly listed the name of the application add and delete sections as [APP_PUBLIC_ADD] and [APP_PUBLIC_DELETE]. The correct naming was [APP_ADD] and [ADD_DELETE].

The MANUAL.CMD file had the incorrect file name for the HP LaserJet file name. The READ.ME was also incorrect.

External aliases were checked by requesting permissions from the domain controller the user was logged into. This version goes directly to the server holding the resource to check its permissions. Therefore, the server name in the alias must be correct for external aliases.

INDEX

Index