Setting Up LANtastic Accounts and Security

Performance Objectives

When you finish this module you will be able to:

- Explain basic network security theory and hardware security.
- Explain the basics of LANtastic security and walk a user through setting up each level of security provided in the NOS.

You will be able to walk a customer through the following:

- Setting up individual accounts and explain the purpose of each access privilege.
- Setting up wildcard accounts.
- Setting up ACL group accounts and assigning users to those accounts.
- Copying, backing up and restoring resources.

Network Security

Picture an estate. Guards sit at all the gates to block out casual passers-by as well as nogoodniks. The guards, if they do a proper job, will demand to see valid identification. They will check the information on the ID to verify that it belongs to the visitor. Then they will check the name against the owner's access list to determine if the visitor should be admitted.

Once inside, a visitor should not be permitted to wander at will. Valuables need to be kept secure behind locked doors. More guards can be posted with special access lists. Better yet, visitors can be guided directly to the only places they are welcome.

In a network, the server is the estate. It wouldn't do to have someone, either mistakenly or maliciously, format the server's hard drive or get access to the company's accounts or leave unwelcome messages to the president inside the Annual Report. There are tried-and-true security precautions that can prevent most of these types of misfortunes. It's good to remember, though, that network security in LANtastic, as well as most PC-oriented local area networks, is a passive affair. No Rottweilers roam behind the walls ready to nab tresspassers. Unless you count the system administrator who might be sitting at the console when a user tries to nab a customer list.

Security precautions for LANs fall into several general categories:

1. Limiting Physical Access

   Most keyboard locks and login passwords can be bypassed simply by booting with a floppy. Even if the floppy drive is physically disabled, a sufficiently knowlegable user can hook into the machine. There is no substitute for physically isolating the machine behind locked doors.

If this is not possible, the next-best alternative is to use a CMOS that has a password lock in its feature set. These can't be bypassed with a floppy and they're obstinate about hacking through the parallel ports. This will also require a key for the box so a hacker can't pull the battery wire and wait for the CMOS to die. This can result in a certain awkwardness, however, if the key gets lost and someone forgets the password.

2. Limiting Network Access

   Login privileges are restricted to users with valid names and passwords.

3. Limiting Resource Access

   Users can use some restricted portions of a hard drive or other server feature but only in a limited fashion.

4. Limiting File Access

   Users can see and perhaps call up particular files but they cannot change them or copy them or rename them.

The Net Manager program controls all of these security features on a server. Access to Net Manager can also be limited by using a name and password.

Preliminary Setup

1. Obtain two computers of 386sx25 class or better equipped with NR2000 adapters.
2. Delete all LANtastic software from the hard drives.
3. Perform a standard DOS install of LANtastic version 6.0 on both machines and configure them as servers. Name the machines SERVER and CLIENT. Do not set up any permanent logins or redirections.
4. On machine SERVER, make two directories off the root, one called REBEL and one called EMPIRE.
5. In the REBEL directory, use COPY CON FILENAME to make the following three files:

FILENAME	CONTENTS
LOCATION.TXT	A galaxy far, far away.
PURPOSE.DOC	Overthrow the empire and make millions of dollars for John Lucas.
SUPRISE.BAT	@echo C3PO diodes are wired backwards.

6. In the EMPIRE directory, use COPY CON FILENAME to make the following two files:

FILENAME	CONTENTS
VADER.TXT	Luke Skywalker's Father
WEAPON.DOC	An invulnerable death star made of the finest paper mache.

7. Use Net Manager to make the following resources:

RESOURCE	TRUE PATH
REBEL	C:\REBEL
EMPIRE	C:\EMPIRE

Access Security -- Wildcard Accounts

Not everyone needs network security. Users with small installations and trusted colleagues usually find thrashing through a nest of login prompts and passwords an irritation rather than a feature. For these users, LANtastic provides a Wildcard account that grants access to anyone who knows the server's machine name. This is the default configuration.

1. At machine SERVER, run NET_MGR and select *Wildcard Account Management*. The asterisk account will be highlighted. Press *Enter*. An ACCOUNT INFORMATION screen will appear.

```
+---------------------------------------------------+
¦ Account Information                                ¦
¦---------------------------------------------------¦
¦                    Name: *                         ¦
¦             Description:                           ¦
¦   Account Modifications: Disallowed                ¦
¦              ACL Groups: none                      ¦
¦     Date Last Logged In: 18-Aug-1994               ¦
¦ Account Expiration Date: none                      ¦
¦                Password: **********                ¦
¦Password Expiration Date: none                      ¦
¦    Renew Password Every: 0 Days                    ¦
¦              Privileges: --------                  ¦
¦Number Concurrent Logins: 255                       ¦
¦             Login Hours: Select to Manage          ¦
¦             ACL Summary: Select to View            ¦
+---------------------------------------------------+
```

2. The operation of each feature will be covered in detail in this module. In the meantime, note the following:

   - The Wildcard account has a maximum of 255 simultaneous logins. This is the largest number that can be entered. Users who need to give more than 255 accounts access to the same server will need to use individual accounts.
   - Account Modifications are disallowed by default. This feature, when enabled, allows a user to make certain changes to their account status via their own terminals. It should not be enabled for Wildcard accounts because one user could make changes that would affect the entire network.
   - There is no password assigned by default. A single password for every user on a network doesn't make much sense, but one can be added if desired.

- There are no Privileges assigned by default. The various account privileges are covered in the training module appropriate to their use. For now, highlight the line and press F1-Help. The Help screen will give you a short summary of each privilege.

3. At machine CLIENT, use *NET SHOW* to verify that autologin is enabled with the user name CLIENT.
4. Log into machine SERVER as follows: `NET LOGIN \\SERVER`
5. Verify using NET SHOW that you are logged into \\SERVER as CLIENT.
6. Log out of SERVER as follows: `NET LOGOUT \\SERVER`
7. Verify using NET SHOW that you are logged out.
8. Log into SERVER again slightly differently:

```
NET LOGIN \\SERVER SKYWALKER
```

9. Now run NET SHOW. Note that you are logged into \\SERVER as SKYWALKER even though your user name is CLIENT.
10. Log out as follows: `NET LOGOUT *`
11. Verify using NET SHOW that you are logged out.
12. At machine SERVER, escape back to the Wildcard Account list, make sure the asterisk is highlighted, then tap the Del key to delete the single asterisk account. Press Enter when prompted to confirm.
13. Press Ins to add a new account. Give it the following settings:

Account name:	REBEL-*
Password:	LIBERTY
Description:	Make one up. Be creative.
Concurrent Logins:	10

14. Escape out to the command prompt.
15. At machine CLIENT, attempt to log in as follows: NET LOGIN \\SERVER
16. You will get the error, "Invalid user name or password."
17. Attempt to log in again, this time using:
NET LOGIN \\SERVER REBEL-LUKE LIBERTY. You will be given access.
18. Log out of machine SERVER.
19. At machine SERVER, delete the REBEL-* account. Escape to the main Net Manager menu.

20. Select Server Startup Parameters, press enter on the path to Server, then select Security and Send ID. The Security Configuration screen appears.

```
+--------------------------------------+
¦ Security Configuration: 1252 bytes   ¦
¦--------------------------------------¦
¦      Send Server ID: DISABLED        ¦
¦      Login Accounts: DISABLED        ¦
¦     Account Servers: DISABLED        ¦
¦Access Control Lists: DISABLED        ¦
¦     File Level ACLs: DISABLED        ¦
¦          Group ACLs: DISABLED        ¦
+--------------------------------------+
```

21. Disable all features then escape out to the command prompt.

22. Reset the server by typing SERVER/REM then SERVER. Make a batch file with these two commands in it. You'll be doing this operation quite a few times.

23. At machine CLIENT, log into machine SERVER as follows: NET LOGIN \\SERVER BOGUS BOGUS. Note that you are given access in spite of the fact that you have no wildcard accounts. What happened? Log out of SERVER.

24. At machine SERVER, run NET_MGR and select Server Startup Parameters then Security and Send ID.

25. Enable Login Accounts. Leave the rest of the selects disabled. Escape back to the command prompt and reset the server.

26. At machine CLIENT, log into SERVER as follows: NET LOGIN \\SERVER BOGUS BOGUS. Note that you are now denied access. This demonstrates that this feature must be enabled at the server before it will become effective.

Access Security -- Individual Accounts

1. Select Individual Account Management. Note that there are no individual accounts by default.

2. Tap Ins and make an individual account with the following settings:

Account Name:	SKYWALKER
Password:	WIMP
Description:	Your choice.
Concurrent Login:	Accept default of 1

3. Once the account is displayed on the list, escape to the command prompt.

4. At machine CLIENT, attempt to log in to SERVER as follows: NET LOGIN \\SERVER SKYWALKER WIMP. You will be given access.

5. At machine SERVER, attempt to log in using the same user name and password. You will get an error, "Too many redirections or logins to network node SERVER. LOGIN has failed." This is caused because you have only one concurrent login on the account.

6. At machine CLIENT, run NET and select *User Account Management.*

7. Select SERVER from the list of servers.

8. The User Account Management screen appears. Select *Switch to New Username*. Enter VADER and no password. You will get an error: "Login Attempt has failed. Invalid user name or password. Press escape."

9. Select Show Account Status. The User Account Status screen appears.

```
+----------------------------------------------------------+
¦ User Account Status for SKYWALKER   on Server \\PRNSERVER ¦
¦----------------------------------------------------------¦
¦               Description:                               ¦
¦       Date Last Logged In: 27-Aug-1994                   ¦
¦   Account Expiration Date: none                          ¦
¦  Password Expiration Date: none                          ¦
¦      Renew Password Every: 0 Days                        ¦
¦                Privileges: --------                      ¦
¦  Number Concurrent Logins: 1                             ¦
¦Time of Day Allowed Logins: _=Login Allowed .=Not Allowed ¦
¦           +-------- am ----------++-------- pm ----------+¦
¦           12  2   4   6   8   10  12  2   4   6   8   10 ¦
¦----------------------------------------------------------¦
¦     Sunday¦______________________________________________¦
¦     Monday¦______________________________________________¦
¦    Tuesday¦______________________________________________¦
¦  Wednesday¦______________________________________________¦
¦   Thursday¦______________________________________________¦
¦     Friday¦______________________________________________¦
¦   Saturday¦______________________________________________¦
+----------------------------------------------------------+
```

10. Look at the information provided in this screen then escape out to the command prompt.

11. At machine SERVER, run NET_MGR and select Individual Accounts.

12. Select SKYWALKER. Change *Account Modifications* to ALLOWED. Escape out to the command prompt.

13. At machine CLIENT, run NET and select *User Account Management* then SERVER. Note that you now have the option to change or disable your password.

14. Select Change Password. You will be prompted for the old password. Enter WIMP then change the password to HERO. Escape out to the command prompt.

15. Log into SERVER using the new password. Note that you are given access.

16. Run NET and select *User Account Management* then SERVER.

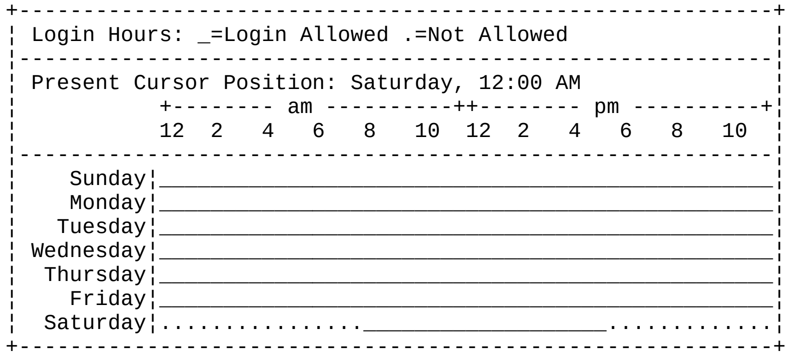
17. Select Disable Account. You will be prompted for your password. Enter HERO. You will not be given a notification that the account is disabled.

18. Select Show Account Status. Note that Concurrent Logins is now set for 0. This is how Net Manager disables an account. Escape out to the command prompt.

19. Log out of SERVER then attempt to log in. You will get the error, "Too many redirections or logins to network node SERVER. LOGIN has failed."

20. At SERVER, run NET_MGR then select Individual Accounts and SKYWALKER. Change the concurrent logins back to 1.

21. Select Login Hours. The Login Hours screen appears.



```
+-----------------------------------------------------------+
¦ Login Hours: _=Login Allowed .=Not Allowed                ¦
¦-----------------------------------------------------------¦
¦ Present Cursor Position: Saturday, 12:00 AM               ¦
¦          +-------- am ----------++-------- pm ----------+¦
¦          12  2   4   6   8   10  12  2   4   6   8   10  ¦
¦-----------------------------------------------------------¦
¦    Sunday¦________________________________________________¦
¦    Monday¦________________________________________________¦
¦   Tuesday¦________________________________________________¦
¦ Wednesday¦________________________________________________¦
¦  Thursday¦________________________________________________¦
¦    Friday¦________________________________________________¦
¦  Saturday¦................__________________..............¦
+-----------------------------------------------------------+
```

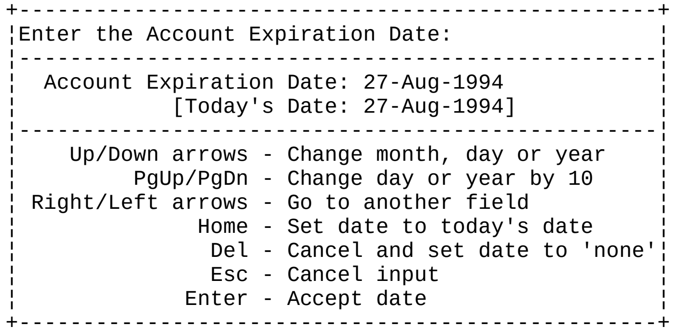
22. Position the cursor on today's day then press the spacebar to change the status as shown in the figure, with access permitted only from 8am to 5pm. Note that you must press Enter to save this change. Do so, then escape out to the command prompt.

23. At machine SERVER, use the DOS TIME command to set the machine's time to 11:00pm.

24. At machine CLIENT, attempt to log into SERVER. You will get an error, "Login attempt invalid at this time. LOGIN has failed."

25. At machine SERVER, use the DOS TIME command to set the machine's time back to normal.

26. Run NET_MGR and select Individual Account and SKYWALKER. Select Account Expiration Date. The Account Expiration Date screen appears.



```
+--------------------------------------------------+
¦Enter the Account Expiration Date:                ¦
¦--------------------------------------------------¦
¦  Account Expiration Date: 27-Aug-1994            ¦
¦            [Today's Date: 27-Aug-1994]           ¦
¦--------------------------------------------------¦
¦    Up/Down arrows - Change month, day or year    ¦
¦         PgUp/PgDn - Change day or year by 10     ¦
¦ Right/Left arrows - Go to another field          ¦
¦              Home - Set date to today's date     ¦
¦               Del - Cancel and set date to 'none'¦
¦               Esc - Cancel input                 ¦
¦             Enter - Accept date                  ¦
+--------------------------------------------------+
```

27. Play with the cursor controls to get the feel for how they change the date then make the expiration date two months prior to the current date. Note that you must press Enter to accept this entry. Do so then escape out to the command prompt.

28. At machine CLIENT, attempt to log into SERVER. You will get the error, "Account has expired, LOGIN has failed."

29. At machine SERVER, run NET_MGR then select Individual Accounts and SKYWALKER.

30. Highlight *Account Expiration Date* and tap the Del key. This will disable the feature. Escape back to the Individual Accounts list.

31. Set up the following individual accounts with default settings and no passwords:

    Lei
    Solo
    Chubaka
    Vader
    Jabba
    Lando
    Imperial_Leader

Resource Security

NOTE: The key to understanding resource security is to keep in mind that a user has access to every directory below the directory to which they have been granted access.

1. Run NET_MGR and select Shared Resources Management.
2. Select the REBEL resource. Cursor down to the Access Control List. Note the asterisk. This wildcard will permit anyone who can log in to have the listed rights for this resource. Note also that the account got all rights by default except for Indirect and Physical. Tap the F1 key for a help screen that contains a short summary of each right. Here is a list:

   R - a file can be opened for reading

   W - a file can be opened for writing

   C - a new file can be created

   M - a new directory can be created

   L - allows a user to do a directory of this resource and see all files. This right is necessary for any other right to be effective.

   D - a file can be deleted

   K - a directory can be deleted

   N - a file can be renamed

   E - an EXE and COM program execution

   A - allow attributes to be changed

   I - allow use of indirect files from this directory

   P - allow direct access to a DOS device
3. Highlight the wildcard account. Tap the Del key. Note that you will get an error message telling you that this account cannot be deleted. The wildcard account is a permanent fixture of any resource.
4. Tap F4-Clear. All the rights disappear. Escape back to the command prompt.
5. At machine CLIENT, log into SERVER as user SOLO.
6. Run NET and select Connect to Other Computers' Drives.

7. Select the R logical drive and pick SERVER from the server list. The Resource List appears. Note that the REBEL resource is on the list with all access rights even though you cleared them all out. Select this resource.
8. Go to the logical drive you redirected and do a directory. Type out the LOCATION.TXT file. You will see that you have full access. Log out of SERVER.
9. At machine SERVER, run NET_MGR and select Server Startup Parameters then Security and Send ID.
10. Enable Access Control Lists. Leave File Level ACLs and Group ACLs disabled. Escape back to the command prompt.
11. Reset the server program.
12. At machine CLIENT, log into SERVER as user SOLO again.
13. Run NET and select Connect to Other Computers' Drives.
14. Select an unused logical drive and pick SERVER from the server list. The Resource List appears. Note that the REBEL resource is no longer visible.
15. Log out of SERVER.
16. At machine SERVER, run NET_MGR and select Shared Resources Management then the REBEL resource.
17. Give the resource the L right then escape back to the command prompt.
18. At machine CLIENT, log into machine SERVER as user SOLO again.
19. Run NET and select Connect to Other Computers' Drives.
20. Select the R logical drive and pick SERVER from the server list. A resource list appears. Note that the REBEL resource is now visible with the L right. Select this resource then escape out to the command prompt.
21. Change to the logical drive you selected and do a directory. You will see the contents of the directory.
22. Attempt to run the SUPRISE.BAT file. You will be denied access.
23. Attempt to make a new file using COPY CON FILENAME. You will be denied access when attempting to close and save the file.
24. Attempt to rename the LOCATION.TXT to LOCATION.NEW. You will be denied access.
25. Attempt to make a new directory called BACKDOOR. You will be denied access.
26. Attempt to type out the contents of LOCATION.TXT. You will be denied access.
27. Attempt to copy LOCATION.TXT to your own hard drive. You will be denied access.
28. Go back to the C drive and log out of SERVER.
29. At machine SERVER, run NET_MGR and select Individual Account Maintenance then account SOLO.

30. Cursor down to Privileges and give the account the A (Super-ACL) privilege. Escape out to the command prompt.

31. At machine CLIENT, log into SERVER as SOLO.

32. Run NET and select Connect to Other Computers' Drives. Select the R logical drive and pick SERVER from the server list. Note that the REBEL resource is on the resource list with all rights. This shows how the Super-ACL privilege bypasses resource security.

33. Escape back to the command prompt and log out of SERVER.

34. At machine SERVER, use Net Manager to:

35. Take the A privilege away from SOLO.

36. Clear the L right from the wildcard account in the REBEL resource.

37. Clear all rights (use F4-Clear) from the EMPIRE resource.

38. At the EMPIRE resource, under the Access Control List, tap the Ins key to add an account to the list. Enter VADER when prompted then escape out to the command prompt.

39. At machine CLIENT, log into SERVER as VADER.

40. Run NET and select Connect to Other Computers' Drives. Select the F drive and pick SERVER from the list of servers.

41. Note that VADER has full access to the EMPIRE resource but cannot see the REBEL resource.

42. Escape out to the command prompt. Redirect your M logical drive to the \\SERVER\C-DRIVE resource.

43. Change to the M drive. Change directory to the REBEL directory. Attempt to run the SUPRISE.BAT file. It will run. This demonstrates that a user with rights to a higher directory will have those same rights in any of the lower directories.

44. Use Net Manger to remove all rights from the C-DRIVE resource.

45. Escape out to the command prompt and proceed to the next section.

ACL Group Accounts

NOTE: Even though ACL stands for Access Control Lists, they do not control initial access to the server. This is strictly a function of the Wildcard or Individual account lists.

1. At machine SERVER, select ACL Group Management. The Defined Group screen appears. Note that there are no default groups.

2. Tap the Ins key to add a new group account. Enter GOOD_GUYS with a description of your choice.

3. Press Enter on the new group name. The ACL Group Information list appears. Note that this list is currently empty.

```
+-------------------------------------+
¦ ACL Group Information               ¦
¦-------------------------------------¦
¦       Name: GOOD_GUYS               ¦
¦Description: Your Choice             ¦
¦                                     ¦
¦-----------Group Members-------------¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
¦                                     ¦
+-------------------------------------+
```

4. Tap the Ins key to add members. A list of individual accounts appears. Highlight SKYWALKER and press Enter. Note that a check mark appears next to that account and the name appears on the Group Members list.

5. Repeat this operation for LEI, CHUBAKA, and SOLO.

6. Escape back to the Defined Groups screen then tap the Ins key to add another group. Enter BAD_GUYS when prompted then escape back to the main Net Manager menu.

7. Select Shared Resources Management then the REBEL resource. Cursor down to the Access Control List. Tap the Ins key to add a new account and enter GOOD_GUYS when prompted. Escape out to the command prompt.

8. At machine SERVER, run NET_MGR and select Individual Account Management then account LEI.

9. Select ACL Summary at the bottom of the Account Information. A resource list appears. Note that LEI has no rights to the C-DRIVE nor the EMPIRE resource but has full rights to the REBEL resource thanks to her membership in the GOOD_GUYS group. She has access to other resources thanks to the wildcard accounts in their Access Control Lists.

```
+-------------------------------------------------------------------+
¦Resource Name                        ACLs     =  Account   +    Groups    ¦
¦-------------------------------------------------------------------¦
¦.                               R---L---E---  R---L---E---  R---L---E--- ¦
¦                                                                   ¦
¦@PRINTER                        RWC-L-------  RWC-L-------  RWC-L------- ¦
¦                                                                   ¦
¦AMAIL                           RWCMLDKNEA--  RWCMLDKNEA--  RWCMLDKNEA-- ¦
¦                                                                   ¦
¦C-DRIVE                         ------------  ------------  ------------ ¦
¦                                                                   ¦
¦AMAILPRG                        RWCMLDKNEA--  RWCMLDKNEA--  RWCMLDKNEA-- ¦
¦                                                                   ¦
¦REBEL                           RWCMLDKNEA--  ------------  RWCMLDKNEA-- ¦
¦                                                                   ¦
¦EMPIRE                          ------------  ------------  ------------ ¦
¦                                                                   ¦
¦                                                                   ¦
¦                                                                   ¦
+-------------------------------------------------------------------+
```

10. At machine CLIENT, log into machine SERVER as LEI. Run NET and select Connect to Other Computers' Drives then pick SERVER from the server list. Note that the C-DRIVE, REBEL, and EMPIRE resources are all missing from the resource list. What happened?

11. At machine SERVER, run NET_MGR and select Server Startup Parameters then Security and Send ID. Enable Group ACLs. Escape out to the command prompt and reset the server.

12. At machine CLIENT, log into machine SERVER as LEI again. Run NET and select Connect to Other Computers' Drives then pick SERVER from the server list. Note that the REBEL resource now is on the list. The C-DRIVE and EMPIRE resources are missing because LEI and her associated account groups have no rights on these resources.

13. Redirect the R logical drive to the \\SERVER\REBEL.

14. Go to the R drive and attempt to run the SURPRISE.BAT file. Note that it runs, verifying that LEI has the rights assigned to her ACL group.

NOTE: *The next few steps are the preferred method for adding individual accounts to a group when using LANtastic version 5.0.*

15. At machine SERVER, run NET_MGR and select Individual Account Management then account VADER.

16. Select ACL Groups on the Account Information screen. The ACL Groups popup appears. It is empty, meaning that this account has not yet been assigned to any groups.

```
+------------------+
¦ACL Groups        ¦
¦------------------¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
¦                  ¦
+------------------+
```

17. Tap the Ins key. A list of Defined Groups appears. Select BAD_GUYS. Note that a check mark appears next to the group, the group members increments to 1, and the group is added to the ACL Group list.

18. Escape back to the Account Information screen. Note that the entry for ACL Groups changes to Select to Manage.

19. Use this same technique to add JABBA, LANDO, and IMPERIAL_LEADER to the BAD_GUYS group.

20. Escape back to the main Net Manager menu.

File Level Security

There are times when it is not possible to divvy up the files between directories to use resource security. In these instances, it is possible to restrict access to certain types of files using file level security.

1. At machine SERVER, use Net Manager to make a new individual account called OBIWAN. Put OBIWAN on the Access Control List of the C-DRIVE resource and let him keep all the default rights. Reset the server.
2. At machine CLIENT, log out of machine SERVER using NET LOGOUT * then log in as OBIWAN. Verify that this account has full access rights to the C-DRIVE resource, including the C:\REBEL and C:\EMPIRE subdirectories.
3. Log out of SERVER.
4. At machine SERVER, run NET_MGR and select Shared Resources Management then the C-DRIVE resource.
5. Select File Security. When prompted for a file name, enter EMPIRE*.*. The File-Level Security screen appears. Note that the filename you entered appears on the left half of the split screen and a wildcard account will full rights appears to the right.

```
+---------------------------+   +------------------------------+
|File-Level Security        |   |Account/Group     ACLs        |
|---------------------------|   |------------------------------|
|\EMPIRE\*.*                |age|*                 RWCMLDKNEA--|
|                           |---|                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
|                           |   |                              |
+---------------------------+   +------------------------------+
```

6. Press Tab to go to the right side of the screen. Tap F4-Clear to remove rights from the wildcard account.
7. Tap Ins to add an account. Enter OBIWAN then use F4 to remove his rights to this subdirectory. Escape out to the command prompt. Reset the server.
8. At machine CLIENT, log into SERVER as OBIWAN. Redirect the M logical drive to \\SERVER\C-DRIVE.
9. Go to the M drive and change to the EMPIRE directory. Do a directory. You will see the directory list. Type out the WEAPON.DOC tile. You will see the contents. What's happened? Log out of SERVER.
10. At machine SERVER, run NET_MGR and select Server Startup Parameters then Security and Send ID. Enable File Level ACLs. Escape out to the command prompt and reset the server.

11. At machine CLIENT, log into SERVER as OBIWAN. Redirect the M logical drive to \\SERVER\C-DRIVE.

12. Go to the M drive and change to the EMPIRE directory. Do a directory. You will see the directory list. Type out the WEAPON.DOC tile. You will be denied access. This demonstrates that file level security must be enabled at the server to make the feature effective.

Using Account Management Utilities

1. If the account information for a new user is similar to an existing account, it can be simpler to copy the that existing account information rather than key it in all over again.

2. At machine SERVER, Run NET_MGR and select Individual Accounts. Highlight SKYWALKER and tap C-Copy. The Copy Accounts screen appears.

```
+---------------------------------------------------+
¦ Copy Accounts                                     ¦
¦---------------------------------------------------¦
¦        From Account: SKYWALKER                    ¦
¦          To Account: R2D2                         ¦
¦To Control Directory: \\SERVER\C-DRIVE\LANTASTI.NET¦
¦            Password: **********                   ¦
¦             Replace: NO                           ¦
+---------------------------------------------------+
```

3. Change the To Account entry to R2D2. Leave all other entries the same. Tap F10-Execute Copy. Escape back to the Individual Accounts list. R2D2 will appear at the bottom of the account list.

4. Press Enter on R2D2 to see the Account Information screen. Note that his account is precisely the same as SKYWALKER's, even to being added to the GOOD_GUYS group.

5. As you may have already noticed, the accounts on this list are kept in the order they were added. As you can imagine, it might be difficult to find a particular account on a server with a large number of users.

6. Tap F-Find and enter LANDO. The highlight will move to the LANDO account. If you play with this feature you will find out it has a few eccentricities.

   - It will not report if a search failed.
   - It only searches from the cursor downward.

7. Another way to make this job easier is to export the account information, manipulate it with a suitable database tool or text editor, then import it back into the control directory.

8. Escape out to the main Net Manager menu. Select Management Utilities then Write Accounts to File. You are presented with three options for file type. Use each option to write a separate file: ACCT1.TXT, ACCT2.TXT and ACCT3.TXT.

9. Escape out to the command prompt then use EDIT to view the text.

   Parameter Data Format -- information for each field is preceeded by the field name. This is the most convenient format for using a text editor.

   Simple Data Format -- information is stored in fixed-sized records with no real hint as to the content. This is only used for database programs that require fixed record sizes.

   Delimited Data Format -- shows account information delimited by "","". This is an Xbase standard and is most useful for using an Xbase program such as Dbase, Foxbase, etc.

10. In module NOS01, Installing LANtastic Network Operating System for DOS and Windows, you learned how important it is to make a backup of the network control directory in case one should become corrupted. If a user has not done so (impossible as it might seem) this it can be handy to copy individual and group accounts on a server so as to simply changing servers or making new control directories.

11. If a user has ACL groups, another way to quickly copy accounts from one control directory to another is to copy the ACL group.

12. At machine SERVER, run NET_MGR and select Control Directory Maintenance. The Control Directory Maintenance menu appears.

13. Select Change Control Directory and type NEW.NET when prompted.

14. When you are returned to the menu, select Create Control Directory. When the program has finished creating the directory, you are returned to the menu. Escape back to the main Net Manager menu. Note that now the column heading reads Managing: C:\NEW.NET.

15. Escape out to the command prompt then run NET_MGR again. You will return to managing the default LANTASTI.NET control directory. Select ACL Group Management.

16. From the Defined Groups list, highlight GOOD_GUYS then tap C-Copy. The Copy ACL Groups screen appears.

```
+----------------------------------------------+
¦ Copy ACL Groups                              ¦
¦----------------------------------------------¦
¦     From ACL Group: GOOD_GUYS                ¦
¦       To ACL Group: GOOD_GUYS                ¦
¦To Control Directory: C:\LANTASTI.NET         ¦
¦           Password: ________                 ¦
¦            Replace: NO                       ¦
+----------------------------------------------+
```

17. Note that you cannot move the cursor up to the To and From fields. This feature can only be used to copy ACL groups between control directories.

18. Press Enter on To Control Directory and enter C:\NEW.NET then tap F10-Execute. When the operation is completed you will remain at the Copy screen. Escape out to the command prompt.

19. Enter the following command: NET_MGR/CONTROL=C:\NEW.NET. The Net Manager menu will appear for the NEW.NET control directory.

20. Use Password Maintenance to make a password of FORCE for this control directory. Escape out to the command prompt.

21. Run NET_MGR as usual, without a command line switch, to manage the default LANTASTI.NET directory.

22. Select ACL Group Management and highlight the BAD_GUYS group.

23. Tap C-Copy and enter the NEW.NET directory in the To Control Directory field.

24. Tap F10-Execute. You will get an error "Invalid password for destination control directory."

25. Highlight Password: and press Enter and change the password to FORCE then tap F10-Execute again. This time the group will copy.

This is the end of this exercise.

Setting up LANtastic Accounts and Security

Training Workbook
Module NOS03
Revision 1.1
2/10/95

ARTISOFT CORPORATE MISSION

To be a leading developer and marketer of network solutions to workgroups, small businesses, and remote network users.

SALES AND SUPPORT MISSION

To establish channel franchises through sales execution, support, and technical services on a global basis.

SALES AND SERVICE DEPARTMENT MISSION

To provide such excellent service to our customers that they will recommend and repurchase our products.

SERVICE AND PRODUCT QUALITY DEPARTMENT MISSION

To provide Artisoft Technical Support and Sales associates with the best training and best information tools in the industry.

PLEASE NOTE: This is a training document. It is not intended for use as a troubleshooting reference. Product features and concerns can and often do change without notice. Please refer to source documents or Folios for the most current product information.