REȚELE LOCALE NOVELL

drnd. asist. Anda Monica Morait

Universitatea București

Rezumat: Prezenta lucrare de sinteză abordează domeniul rețelelor locale Novell și, în special, sistemul de operare NetWare 3.11. În cuprinsul ei sunt tratate conceptele de bază ale rețelelor locale Novell: componentele software, securitatea datelor în rețea, tipuri de utilizatori și de utilitare, accesul pe directoare și mapări de drivere.

O parte însemnată a lucrării este dedicată celor 4 niveluri de securitate într-o astfel de rețea, ce permit protecția datelor, astfel încât o rețea de calculatoare să devină un mediu organizat și sigur, care să servească cerințele utilizatorului. De asemenea sunt prezentate resursele partajabile ale rețelei : discul hard al file serverului - structura sa de directoare, datele, aplicațiile, imprimantele de rețea, ș.a.m.d., precum și tipurile de utilizatori care pot accesa aceste resurse.

Cuvinte cheie: LAN Novell, file server, stație de lucru, NetWare, supervizorul rețelei, securitatea datelor în rețea, securitatea la login, drepturi acordate (TA), masca drepturilor moștenite (IRM), drepturi efective, atribute, mapări de drivere, driver local, driver de rețea, driver de căutare, login script.

O rețea locală Novell (Novell Local Area Network sau Novell LAN) este un grup de computere (de ex. IBM-PC sau Macintosh), ce sunt legate împreună, astfel încât să poată comunica și să-și partajeze resursele. O astfel de rețea este alcătuită din stații de lucru, periferice și unul sau mai multe file servere. Fiecare din utilizatorii rețelei, lucrând pe un computer personal conectat la aceasta, poate comunica cu fiecare din ceilalți utilizatori din rețea. Ei pot, de asemenea, să partajeze resursele rețelei (discul hard al file serverului, datele, aplicațiile, precum și imprimantele de rețea) și să utilizeze orice servicii dintre cele oferite de rețea.

Un LAN NOVELL are două componente soft de bază:

1. Sistemul de operare NetWare
2. Sistemul de operare local al stației (ex. MS-DOS)

Sistemul NetWare este încărcat în memoria file serverului, permițând acestuia să reglementeze comunicația între computerele atașate rețelei și să gestioneze resursele partajabile ale rețelei. Cerințele minime ca un calculator să poată deveni file server și să ruleze sistemul NetWare sunt de cel puțin: un hard disc, 4 MB memorie RAM și o placă de rețea instalată.

Există două tipuri de file servere: nedecicate și dedicate. File serverul nedecicat permite utilizarea sa atât ca file server, cât și ca stație de lucru, executând atât sistemul de operare al rețelei, cât și aplicații ale utilizatorilor. File serverul dedicat va executa numai sistemul de operare NetWare.

Sistemul de operare local al stației este, de obicei, o versiune a sistemului de operare MS-DOS sau OS/2.

Pentru comunicarea cu file serverul, stația de lucru are 2 parți software:

1. shell-ul
2. protocolul de comunicație

Shell-ul este încărcat în RAM-ul stației de lucru ca program TSR (Terminate-and-Stay-Resident). El direcționează cererile stației către sistemul de operare local sau către file serverul rețelei pentru a fi servite de către sistemul de operare NetWare, depinzând de tipul acestor cereri. Prin urmare, când o stație face o cerere, shell-ul va decide dacă este un "task" de rețea pentru trimitere la NetWare sau unul local pentru a fi preluat de sistemul de operare local (figura 1). Shell-ul este conținut în programul NETx.COM (unde x reprezintă versiunea sistemului de operare local MS - DOS).

Protocolul de comunicație este limbajul pe care stația de lucru îl utilizează pentru a comunica cu file serverul și este conținut în programul IPX.COM. (IPX.COM este creat prin execuția programului WSGEN.EXE). Shell-ul utilizează acest protocol pentru a trimite cererile către NetWare, deci, către file server.

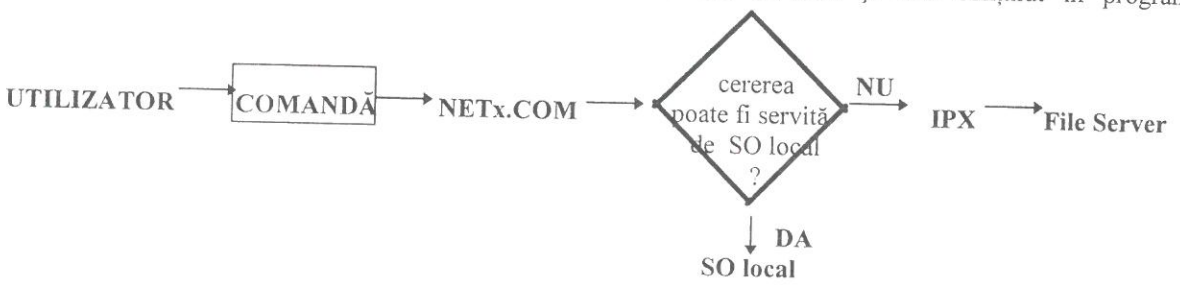


Figura 1.

În concluzie, un computer "standalone" poate deveni stație de lucru adăugându-i-se o placă de rețea și încărcând cele două fișiere ce conțin programele rezidente: NETx.COM și IPX.COM.

1. Nivelurile structurii de directoare NetWare

Structura de directoare este utilizată pentru a organiza fişierele pe hard-discul file serverului.

Primul nivel al structurii îl reprezintă **VOLUMUL** care este echivalent cu directorul rădăcină din structura de directoare DOS. Următorul nivel îl constituie directoarele, ce conţin fişiere şi/sau subdirectoare. Numele file serverului va fi specificat înaintea numelui volumului, numai pentru a diferenţia volume cu acelaşi nume din sisteme cu mai multe servere.

Observaţie

Volumul fiind o unitate logică, el poate conţine mai multe unităţi fizice de disc.

În reţea, specificarea completă a unei căi se face indicând numele file serverului, al volumului şi "calea" de nume de directoare ce conduce la subdirectorul, respectiv fişierul dorit. Se vor utiliza următoarele convenţii când se specifică o "cale" director:

File_Server/Volum:Director/SubDirector[/Nume_Fişier]

unde: file_server, volum şi director se înlocuiesc cu numele acestora din structura de directoare. Fiecare dintre aceste nume poate avea între 1 şi 8 caractere. Deşi DOS recunoaşte numai caracterul backslash (\), ca separator al nivelurilor structurii, NetWare recunoaşte atât caracterul slash (/), cât şi backslash (\). Însă, volumul şi primul director după volum trebuie separate prin caracterul (:). "Calea" poate conţine opţional şi un nume de fişier.

În cursul procesului de instalare, NetWare creează automat un set de directoare şi fişiere în volumul SYS:

- directorul SYS:LOGIN ce conţine programele necesare pentru conectarea la file server;

- directorul SYS:SYSTEM ce este utilizat pentru administrarea sistemului, conţinând fişierele sistemului de operare, utilitare NetWare şi programe rezervate pentru supervizorul sistemului;

- directorul SYS:PUBLIC care este un director pentru acces general, conţinând utilitare NetWare şi programe pentru toţi utilizatorii din reţea;

- directorul SYS:MAIL ce conţine pentru fiecare utilizator recunoscut de file server, câte un subdirector având acelaşi nume cu identificatorul utilizatorului din Bindery (User Identifier (ID)). Un astfel de subdirector va conţine login scriptul individual şi configuraţiile joburilor de tipărire la imprimanta de reţea.

În afara acestor directoare create automat, supervizorii reţelei sunt responsabili cu crearea unei structuri de directoare în acord cu necesităţile din reţea. Astfel, se recomandă crearea următoarelor directoare pentru a îmbunătăţi organizarea fişierelor şi pentru a seta mai uşor parametrii pentru protecţia informaţiei (drepturi, atribute):

- Unul sau mai multe directoare DOS: Pentru fiecare versiune a sistemului de operare MS-DOS utilizată pe staţiile de lucru, trebuie creat câte un director.

- Unul sau mai multe directoare pentru aplicaţii.: Se va crea câte un director separat pentru fiecare aplicaţie, ce va conţine numai fişierele aplicaţiei respective. Fişierele sursă, create de utilizator, nu vor fi stocate în acest director, utilizatorii neavând acordate drepturi de scriere sau ştergere în director.

- Un director "home" sau "nume utilizator" pentru fiecare utilizator: Fiecare utilizator trebuie să aibă câte un director propriu de lucru în care să-şi stocheze fişierele sursă create. În aceste directoare, utilizatorii vor avea acces complet astfel încât să-şi poată salva fişierele sau crea subdirectoare pentru a-şi organiza propriile fişiere. Astfel, într-un director "home" utilizatorul va avea toate drepturile: [SRWCEMFA]. În general, directoarele "home" au acelaşi nume cu numele de conectare ale utilizatorilor, pentru uniformitate şi uşurinţă la crearea Login Script-urilor.

- Un director comun care să servească ca punct intermediar în transferuri de date ("Shared Data Area")

2. Utilitarele reţelei

Într-o reţea NetWare există 5 tipuri de utilitare:

- comenzi consolă

- module încărcabile

- utilitare linie de comandă

- utilitare cu meniu

- fişierul executabil -->**SERVER.EXE**.

Fiecare tip are un indicativ ("icon") pentru o identificare mai uşoară.

Comenzile consolă

Indicativul [:] marchează comenzile consolă.

Comenzile consolă sunt parte a programului **SERVER.EXE** ce este executat pentru instalarea

sistemului NetWare v.3.11 pe file server. După rularea acestui program, se pot executa diferite "task"-uri de instalare şi întreţinere, lansând aceste comenzi de la consola file serverului (de exemplu: **BIND** - pentru a lega drivere de LAN la un protocol de comunicaţie şi la o anumită placă de reţea, **LOAD** - pentru a lega module încărcabile cu sistemul de operare **MOUNT** - pentru a face un volum disponibil utilizatorilor reţelei). De asemenea, se pot lansa de la consola file serverului comenzi ecran (cum ar fi: **BROADCAST** - pentru a trimite un mesaj de la consola file serverului utilizatorilor conectaţi la acesta; **CLS** - pentru a şterge ecranul file serverului) şi comenzi pentru afişarea unor informaţii cu privire la configuraţia file serverului (de exemplu: **DISPLAY NETWORKS; DISPLAY SERVERS; PROTOCOL; SPEED; VERSION; VOLUMES** şamd).

Majoritatea comenzilor consolă sunt în partea internă a sistemului de operare. Alte comenzi consolă se pot lega cu sistemul de operare când se încarcă un modul încărcabil. (De exemplu: când se încarcă modulul **UPS.NLM,** se adaugă două noi comenzi consolă la sistemul de operare: **UPS STATUS** şi **UPS TIME**.)

Comenzile consolă se pot introduce numai de la prompterul consolei file serverului [:].

Module încărcabile

Indicativul **[:LOAD]** marchează modulele încărcabile, ce leagă la sistemul de operare drivere de disc, drivere LAN, alte utilitare pentru prelucrarea şi creşterea performanţelor file serverului. Modulele încărcabile (NetWare Loadable Modules (NLMs)) sunt programe care se pot încărca şi descărca din memoria FS-ului în timp ce acesta merge. NetWare are patru tipuri de module încărcabile:

- drivere de disk care controlează comunicaţia între sistemul de operare şi hard discurile: ele au extensia **.DSK**;
- drivere de LAN care controlează comunicaţia între sistemul de operare şi plăcile de interfaţă pentru reţea: ele au extensia **.LAN**;
- utilitare de administrare şi module care permit monitorizarea şi schimbarea opţiunilor de configurare: ele au extensia. **NLM**;
- module cu extensia **.NAM** (Name Space Modules): un astfel de modul permite stocarea fişierelor ce nu sunt de tip MS-DOS pe file serverul ce rulează NetWare.

Utilitarele linie de comandă

Indicativul **[F>]** marchează utilitarele linie comandă în NetWare. Ele se execută ca linii de comandă pe staţiile de lucru şI le îndeplinesc diferite "task"-uri în reţea:

- vizualizare liste de fişiere, directoare, file servere, utilizatori, drepturi utilizatori;
- copiere şi tipărire fişiere;
- mapări de drivere de reţea;
- adăugare / revocare drepturi;
- conectare / deconectare la / de la file server.

Dacă sunteţi familiarizaţi cu utilitarele linie de comandă, acestea sunt mai uşor de utilizat şi mai rapide decât utilitarele cu meniu.

Utilitarele cu meniu

Se folosesc pentru a executa "task"-uri în reţea prin alegerea unor opţiuni din meniuri. Ele se execută tot pe staţiile de lucru. Anumite "task"-uri în cadrul utilitarelor cu meniu pot fi executate numai de supervizori sau utilizatori care au cont echivalent supervizor. Deşi majoritatea operaţiilor în reţea pot fi realizate atât de utilitarele linie de comandă, cât şi de utilitarele cu meniu, totuşi, unele dintre acestea, se pot executa numai din utilitarele cu meniu.

Fişierul executabil SERVER.EXE

Indicativul **[A>]** marchează fişierul SERVER.EXE. El "boot"-eaza sistemul de operare NetWare pe *file server* şi se poate executa din:

- partiţia DOS de pe driverul C al file serverului;
- driverul A.

După execuţia SERVER.EXE se pot încărca driverele de disc şi driverele de LAN pentru configurarea completă a sistemului de operare. După configurare, se pot introduce comenzi consolă sau module încărcabile pentru întreţinerea şi monitorizarea activităţii în reţea.

3. Tipuri de utilizatori în reţea

Pentru a i se permite unei persoane să lucreze în reţea, aceasta trebuie să fie un utilizator recunoscut în reţea, deci, să aibă atribuit un nume care să fie un obiect al aşa-numitului "Bindery" de pe file server. Bindery reprezintă o bază de date, orientată obiect care conţine definiţii cu privire la entităţi cum ar fi: utilizatori, grupuri de utilizatori etc. Ea are trei componente:

1. **obiectele** - sunt memorate în fişierul NET$OBJ.SYS;
2. **proprietăţile** - sunt memorate în fişierul NET$PROP.SYS;

3. **valorile proprietăților** - conținute în fișierul NET$VAL.SYS.

Obiectele reprezintă orice entitate logică sau fizică cum ar fi: utilizatori, grupuri de utilizatori, file ser-vere, print servere sau orice altă entitate căreia i se dă un nume. **Proprietățile** sunt caracteristicile fiecărui obiect din Bindery, cum ar fi: parole, restricții de cont, lista membrilor grupului, drepturi asignate. **Valorile proprietăților** sunt valorile atribuite proprietăților obiectelor. Astfel, Bindery permite supervizorului rețelei să proiecteze un mediu organizat și sigur care să conțină cerințele specifice fiecărei entități.

Un utilizator autorizat capătă acces la resursele file serverului prin execuția programului LOGIN. Când un utilizator a inițiat o cerere de conectare, programul LOGIN.EXE citește întâi fișierul NET$OBJ.SYS pentru a verifica dacă numele său figurează în lista de obiecte din Bindery, determinând astfel dacă utilizatorul respectiv este un utilizator recunoscut în rețea. Dacă un obiect cu acest nume există, programul LOGIN.EXE va citi fișierul NET$PROP.SYS ce conține proprietățile asociate obiectelor, în acest caz pentru a vedea dacă proprietatea parolă există pentru obiectul respectiv. Dacă proprietatea parolă există, utilizatorului i se va cere de la prompter. Programul LOGIN va compara valoarea introdusă de utilizator cu cea conținută în fișierul NET$VAL.SYS. Dacă aceste două valori se potrivesc, utilizatorului i se permite accesul la resursele file serverului în conformitate cu valorile setate pentru alte proprietăți care există pentru acesta (cum ar fi: restricții de cont și drepturi acordate).

Există cinci tipuri de utilizatori în rețea:

- supervizorii sau administratorii de sistem
- operatorii consolă
- administratorii de grup ai sistemului
- administratorii contului utilizatorilor
- utilizatorii obișnuiți

Supervizorii sau administratorii de sistem

Aceștia se pot conecta cu numele recunoscut în rețea: SUPERVISOR. Un utilizator supervizor are toate drepturile în toate directoarele. Aceste drepturi nu pot fi revocate, iar contul SUPERVISOR nu poate fi șters sau redenumit. Contul SUPERVISOR este obiectul din BINDERY având numărul de identificare utilizator (USER IDENTIFIER (ID)) 1. (ID unui utilizator reprezintă "semnătura" utilizatorului din Bindery și îl regăsim ca nume de subdirector în <MAIL>).

Utilizatorii obișnuiți

Sunt persoane ce execută aplicații în rețea, accesând fișiere de pe file server în acord cu drepturile acordate.

Operatorii consolă

Sunt utilizatori cărora supervizorul le-a acordat dreptul să folosească utilitarul FCONSOLE. Acest utilitar permite operatorului consolă să trimită mesaje utilizatorilor, să schimbe file serverele, să acceseze informația de conectare, să vizualizeze informația cu privire la versiunea NetWare, să schimbe data și timpul sistemului, să activeze sau să dezactiveze conectarea utilizatorilor suplimentari, să activeze sau să dezactiveze sistemul tranzacțional (Transaction Tracking System - TTS).

Administratorii de grup (Workgroup Manager)

Sunt utilizatori ce au primit dreptul de a crea obiecte în Bindery (cum ar fi utilizatori și grupuri de utilizatori) și de a administra conturile utilizatorilor creați.

Administratori ai contului utilizatorilor (User Account Manager)

Acești utilizatori pot administra conturi, dar nu pot crea obiecte în Bindery. Ei pot realiza toate ope-rațiile corespunzătoare opțiunilor din submeniul "User Information" al utilitarului SYSCON, cu excepția celor referitoare la drepturile acordate în directoare și fișiere și restricții de spațiu pe disc. Deci, vor putea vizualiza și modifica următoarele informații cu privire la utilizatorul al cărui cont îl administrează:

- starea contului - opț. *Account Balance*;
- restricții impuse la conectare - opț. *Account Restrictions*;
- -schimbarea parolei (nu și vizualizarea acesteia) - opț. *Change Password;*
- numele întreg sau descriptorul de nume - opț. *Full Name*;
- grupurile în care utilizatorul selectat este membru - opț. *Groups Belonged To* (va putea modifica această informație doar dacă este și administrator al grupului respectiv);
- login scriptul utilizatorului selectat - opț. *Login Script;*
- utilizatori și grupuri administrate - opț. *Managed Users and Groups;*
- administratori - opț. *Managers;*
- lista utilizatorilor de la care a primit drepturi prin securitate echivalentă - opț.*Security Equivalences*
- restricții de conectare de la anumite stații - opț. *Station Restriction;*
- restricții de timp - *Time Restriction.*

După instalarea SO NetWare pe file server vor exista în BINDERY două conturi (SUPERVISOR şi GUEST) şi grupul EVERYONE. GUEST este un utilizator obişnuit în reţea, ce are acces limitat la resursele file serverului şi este membru al grupului EVERYONE. Deoarece după instalarea FS atât contul SUPERVISOR, cât şi GUEST nu sunt protejate prin parolă, se recomandă parolarea acestor conturi de la primul login. Grupul EVERYONE este un grup special, deoarece orice utilizator creat va deveni automat membru al acestui grup. Grupului EVERYONE îi sunt asignate automat drepturile Read şi File Scan în directorul SYS:PUBLIC şi dreptul Create în SYS:MAIL. Supervizorul de reţea poate şterge orice utilizator din acest grup sau să schimbe drepturile acordate grupului EVERYONE în orice director.

Observaţii

1. Nu se recomandă ştergerea drepturilor grupului EVERYONE din SYS:PUBLIC şi SYS:MAIL, deoarece utilizatorii îşi vor pierde în acest mod dreptul de acces la utilitarele de reţea, respectiv la poşta electronică.
2. Grupul EVERYONE este obiect în BINBERY. Odată şters şi apoi recreat, îşi va pierde caracteristica de a include automat ca membru al său pe orice utilizator nou creat; în acest caz, utilizatorii, pentru a deveni membri ai acestui grup, vor trebui în mod explicit adăugaţi grupului, unul câte unul.

4. Securitatea datelor în reţea

Toate informaţiile în reţea sunt depuse pe hard discul file serverului, astfel că una dintre problemele importante ce se pune la nivelul unei reţele de calculatoare este cea a protecţiei datelor.

Securitatea în reţea este organizată pe patru niveluri:

1. securitatea la login,
2. drepturi acordate utilizatorilor,
3. atributele fişierelor şi directoarelor,
4. securitatea la file server.

Astfel, securitatea NetWare va controla:

1. cine poate accesa reţeaua,
2. ce directoare şi fişiere pot accesa utilizatorii,
3. ce operaţii le sunt permise utilizatorilor în aceste directoare şi fişiere,
4. cine poate executa operaţii de la consola file server-ului.

Securitatea la login

Controlează accesul iniţial la reţea.

Supervizorul reţelei va stabili elementele primului nivel de securitate prin:

- definirea utilizatorilor,
- dând (opţional) posibilitatea de protejare a contului prin parolă,
- setând restricţii la conectare.

Definirea utilizatorilor

Numai supervizorii de reţea şi administratorii de grup pot crea utilizatori. Numele utilizatorilor creaţi sunt memorate în baza de date orientată pe obiecte, numita **Bindery** şi le sunt atribuite proprietăţi (cum ar fi: parola, restricţii de cont, drepturi acordate) . Pentru a accesa file serverul, un utilizator trebuie să-şi cunoască numele de conectare si parola (dacă contul său a fost protejat prin parolă).

Protejarea contului prin parolă

Deşi este opţională, parola este necesară, deoarece orice persoană care a detectat un nume de utilizator valid si neprotejat prin parolă, va putea avea acces la resursele file serverului. De altfel, NetWare asigură confidenţialitatea parolei: când este tipărită de la staţie, ea nu va fi afişată pe monitor. Sistemul codifică parola şi o va memora în această formă pe hard discul file serverului.

Restricţiile la conectare

Controlează când şi unde un utilizator se poate conecta, protejând reţeaua de intruşi. Se pot utiliza următoarele trei tipuri de restricţii la conectare:

- *restricţiile la staţii* limitează conectările concurente (numărul fizic de staţii de la care un utilizator poate executa concurent LOGIN). De asemenea, se poate restrânge dreptul de conectare al unui utilizator de la anumite staţii din reţea (în acest caz, utilizatorul se va putea conecta doar de la staţiile ale căror adrese de nod au fost explicit specificate);
- *restricţiile de timp* limitează intervalul de timp de conectare. O cerere de conectare în afara timpului permis va fi rejectată;
- *blocarea contului* unui utilizator se poate face dacă au fost depăşite anumite limite, cum ar fi: acesta a atins valoarea minimă a creditului (dacă sistemul de contabilitate în reţea este activ), dacă contul a expirat sau a fost dată parola incorect de un număr de ori mai mare decât cel setat.

Drepturi acordate

Al doilea nivel de securitate controlează accesul unui utilizator în anumite directoare sau fişiere şi operaţiile ce îi sunt permise respectivului utilizator în acestea. El este implementat prin :

1. Trustee Assignments (TA)
2. Inherited Rights Masks (IRM)

Trustee Assignments (TA)

Reprezintă drepturile acordate unui utilizator (grup de utilizatori), ce îi vor permite accesul la un fişier sau director numai într-un anumit mod (de exemplu, numai citirea sau execuţia unui fişier fără posibilitatea de ştergere sau scriere în fişierul respectiv).

Masca drepturilor moştenite **(IRM)**

Este dată pentru fiecare director sau fişier când acesta este creat. IRM pentru un director controlează ce drepturi efective pe care utilizatorul le are în directorul părinte le poate "moşteni" şi în directorul respectiv (fiu al părintelui). IRM pentru un fişier controlează ce drepturi ale utilizatorului în director vor fi "moştenite" de fişierul respectiv.

TA şi IRM vor determina *drepturile efective*, adică drepturile pe care un utilizator le poate efectiv exercita într-un anumit fişier sau director. Atât TA, cât şi IRM folosesc acelaşi set de 8 drepturi pentru a controla accesul în directoare şi fişiere. Fiecare drept este reprezentat prin iniţiala sa:

S - Supervisory R - Read W - Write C - Create E - Erase M - Modify F - File Scan A - Access Control

Utilitarele de reţea afişează drepturile prin iniţialele lor între paranteze drepte: **[SRWCEMFA].**

Prin convenţie, absenţa unui drept prin neacordarea sau revocarea sa, va fi indicată printr-un blank în locul iniţialei: [R F].

Fiecare dintre aceste drepturi vor avea înţeles şi efect diferit dacă sunt acordate în fişiere sau în directoare.

Drepturile acordate la nivel de director

Controlează accesul general în director, subdirectoarele şi fişierele sale. Când anumite drepturi sunt acordate la nivel de director, ele se aplică în toate subdirectoarele şi fişierele sale, cu excepţia cazului în care acestea au fost redefinite la nivel de subdirector (fişier) sau au fost revocate din mască (IRM).

Supervisory Utilizatorul are toate drepturile în director, precum şi în toate subdirectoarele şi fişierele acestuia. Dreptul de Supervisory anulează orice restricţie definită prin IRM în subdirectoarele sau fişierele directorului. Utilizatorii care au acest drept îl pot acorda şi altor utilizatori în acel director, respectiv în subdirectoarele şi fişierele sale. Acest drept odată acordat, nu va putea fi revocat decât din directorul în care a fost definit, nu şi din nivelurile inferioare (fişiere sau subdirectoare).

Read Dreptul de a deschide fişierele din director şi de a le citi conţinutul sau executa.

Write Dreptul de a deschide fişierele din director şi de a le modifica conţinutul.

Create Dreptul de a crea subdirectoare şi fişiere în director. De asemenea, utilizatorul va avea dreptul să copieze subdirectoare sau fisiere în directorul respectiv.

Erase Dreptul de a şterge directorul, subdirectoarele şi fişierele acestuia.

Modify Dreptul de a modifica atributele directorului, subdirectoarelor şi fişierelor sale. De asemenea, va avea dreptul de a redenumi directorul, respectiv subdirectoarele sau fişierele sale. Acest drept nu permite modificarea conţinutului fişierelor.

File Scan Dreptul de a afişa intrările din director.

Access Control Dreptul de a modifica TA şi IRM directorului, subdirectoarelor şi fişierelor sale. Utilizatorii ce au acest drept pot acorda la rândul lor orice drept (cu excepţia celui de Supervisory) altor utilizatori în director, respectiv în subdirectoarele şi fişierele sale.

Pentru a acorda sau modifica TA se folosesc utilitarele NetWare: **SYSCON; FILER; GRANT; REMOVE; REVOKE.**

Pentru a modifica IRM pentru directoare se utilizează: **FILER; ALLOW.**

Drepturile acordate la nivel de fişier

Controlează accesul la anumite fişiere din director. Ele se acordă pentru a redefini drepturile pe care utilizatorii le moştenesc din director.

Supervisory Se acordă toate drepturile vizavi de accesul la respectivul fişier. Utilizatorii ce au acest drept vor putea acorda altor utilizatori orice drept în acest fişier.

Read Dreptul de a deschide fişierul şi de a-i citi conţinutul.

Write Se acordă dreptul de a deschide fişierul şi de a-i modifica conţinutul.

Create Dreptul de a restaura fişierul după ce acesta a fost şters.

Erase Dreptul de a şterge fişierul.

Modify Dreptul de a schimba atributele fişierului şi de a-l redenumi. Acest drept nu permite modificarea conţinutului fişierului.

File Scan Dreptul de a vedea numele fişierului la o scanare a directorului. Acordat

împreună cu **Read** va permite execuția unui fișier de tip .EXE sau .COM .

Access Control Dreptul de a modifica TA și IRM pentru respectivul fișier. Cei ce au acest drept pot acorda altor utilizatori orice drept (cu excepția celui de Supervisory) în acest fișier.

Comenzile cu care se acordă sau se modifică TA în fișiere:

SYSCON; FILER; GRANT; REVOKE; REMOVE.

Comenzile cu care se modifică IRM pentru fișiere: **ALLOW; FILER.**

Drepturile efective

Sunt drepturile pe care un utilizator le poate efectiv exercita într-un anumit director sau fișier. Pentru a determina drepturile efective ale unui utilizator, trebuie cunoscut:

- Ce TA au fost acordate acelui utilizator;
- Ce TA au fost acordate grupului din care face parte acel utilizator;
- IRM pentru directorul sau fișierul respectiv.

Dacă au fost acordate TA atât grupului, cât și utilizatorului la un anumit nivel, atunci drepturile efective ale utilizatorului la nivelul respectiv vor fi suma TA ale grupului și ale utilizatorului.

Comenzile cu care utilizatorii pot să-și vizualizeze drepturile efective sunt:

FILER; RIGHTS; WHOAMI.

În rezumat, principiile ce guvernează modul de determinare a drepturilor efective sunt:

1. Dacă S este un drept efectiv în directorul părinte, drepturile efective în director vor fi toate drepturile;
2. Dacă S nu este un drept efectiv în directorul părinte atunci:

   2.1 Dacă în directorul respectiv au fost acordate TA, atunci drepturile efective vor fi drepturile acordate prin TA.

   2.2 Dacă în director nu au fost acordate TA, atunci:

   2.2.1 Dacă masca drepturilor moștenite (IRM) pentru acest director este completă ([SRWCEMFA]), atunci drepturile efective în director vor fi drepturile efective pe care utilizatorul le are în directorul părinte

   2.2.2 Dacă din mască au fost revocate drepturi, atunci drepturile efective în director vor fi filtrate de mască (drepturile efective în director vor fi drepturile efective în directorul

OPERAȚII	DREPTURI NECESARE
Să deschidă fișierul și să-l citească.	Read (*)
Să vadă numele fișierului.	File Scan
Să afișeze intrările în director.	File Scan
Să deschidă și să scrie în fișiere.	Read, Write, Modify (*,**)
Să execute un fișier de tip .EXE (.COM)	Read, File Scan
Să creeze și să scrie în fișierul deschis	Create
Să copieze fișiere din directoare	Read, File Scan
Să copieze fișiere într-un director	Create
Să creeze un nou director	Create
Să șteargă un fișier	Erase
Să restaureze fișierele șterse	Read, Write, Create, File Scan în fișier și Create în
Să schimbe atributele directorului sau ale fișierului	Modify
Să redenumească fișierul sau directorul	Modify
Să schimbe IRM sau TA	Access Control (***)
Să vadă numele directorului	Oricare din cele 8 drepturi în director sau fișie

părinte din care se anulează drepturile ce nu se găsesc în IRM).

Observație

Acordarea drepturilor trebuie făcută cu mare atenție. Dacă un utilizator a primit mai multe drepturi decât cele necesare, acesta va putea șterge, corupe sau sustrage date. În caz contrar însă, el nu va putea să-și execute aplicația. Astfel, dacă unui utilizator i s-a acordat numai dreptul de Read si File Scan, fără a cunoaște dacă aplicația sa creează fișiere temporare când este accesată, atunci acest utilizator ar putea fi împiedicat să-și ruleze aplicația pentru că drepturile C,E și M nu i-au fost acordate.

Pentru ca un utilizator să poată executa următoarele operații, el trebuie să aibă drepturile:

(*) - În general, se acordă împreună cu dreptul de a vedea numele fișierului.

(**) - Modify nu este întotdeauna necesar. (Dacă fișierul are atributul Read Only, utilizatorul nu va putea scrie în fișier chiar dacă are dreptul Write. Având însă dreptul Modify, va putea anula atributul respectiv).

(***) - Nu poate acorda sau revoca dreptul de Supervisory.

Pe cât posibil, este de dorit separarea fișierelor sursă create de utilizator într-o aplicație, de fișierele executabile care sunt necesare rulării aplicației. În acest caz, utilizatorii vor avea nevoie de drepturile Read și File Scan în directorul în care se găsesc fișierele executabile ale aplicației și drepturile de Read, File Scan, Create, Erase și Modify în directoarele în care își crează fișierele sursă.

Drepturi acordate implicit

La instalarea sistemului de operare sunt create automat următoarele obiecte în Bindery: utilizatorul SUPERVISOR, utilizatorul GUEST și grupul EVERYONE.

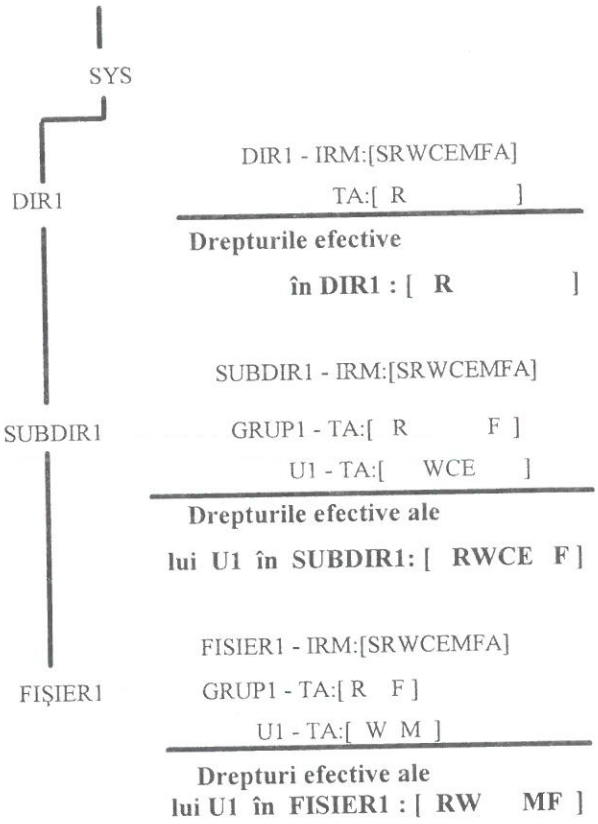
Utilizatorul SUPERVISOR are toate drepturile în toate directoarele.

Utilizatorul GUEST are drepturile derivate din calitatea lui de membru al grupului Everyone.

Grupul EVERYONE are în mod implicit acordate următoarele drepturi de lucru: Create în SYS:MAIL; Read și File Scan în SYS:PUBLIC.

Exemple:

1. Dacă există TA acordate într-un director sau fișier, acestea vor anula atât masca drepturilor moștenite (IRM) pentru acel director, respectiv fișier, cât și drepturile efective din directorul părinte. Deci, drepturile acordate în TA la un anumit nivel = drepturile efective ale utilizatorului la nivelul respectiv.



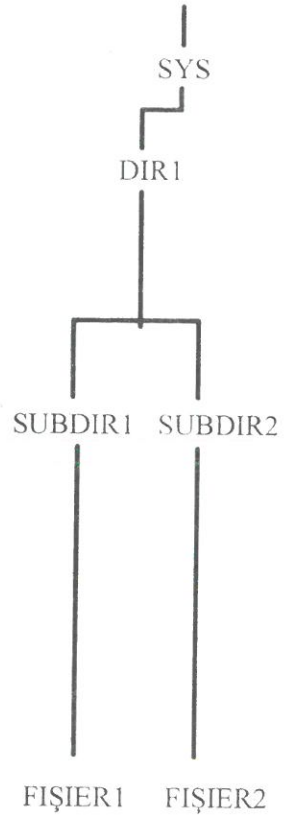
Deoarece utilizatorul U1 are acordate la nivelul SUBDIR1 următoarele TA: Write, Create și Erase, iar grupul din care face parte are Read și File Scan, suma acestor drepturi va reprezenta drepturile efective ale utilizatorului U1 în subdirectorul SUBDIR1.

Observație

Având acordate drepturi în SUBDIR1, utilizatorul U1 va avea și dreptul de File Scan în DIR1, dar limitat, în sensul că va vedea numai subdirectorul SUBDIR1, la o scanare a directorului DIR1.

Dacă au fost acordate TA într-un fișier, drepturile efective sunt determinate în același mod ca și pentru director, anume: TA existente în fișier vor anula drepturile efective din directorul părinte și IRM-ul pentru acel fișier. Drepturile efective ale utilizatorului în fișier vor fi suma TA ale grupului și ale utilizatorului în fișierul respectiv.

2. Cum se determină însă drepturile efective ale utilizatorului dacă acesta nu a primit noi TA la un anumit nivel? Masca Drepturilor Moștenite (IRM) va determina ce drepturi efective din directorul părinte va putea moșteni utilizatorul.



DIR1 - IRM:[SRWCEMFA]
TA:[RWCE F]

Drepturile efective
ale lui U1 în DIR1: [RWCE F]

SUBDIR1 - IRM:[SRWCEMFA]
SUBDIR2 - IRM:[SR F]

Drepturile efective ale
lui U1 în SUBDIR1: [RWCE F]
Drepturile efective ale
lui U1 în SUBDIR2: [R F]

FIŞIER1 - IRM:[SRWCEMFA]
FIŞIER2 - IRM:[R]

Drepturile efective ale
lui U1 în FIŞIER1: [RWCE F]
Drepturile efective ale
lui U1 în FIŞIER2: [R]

Pentru a calcula drepturile efective în SUBDIR1 şi SUBDIR2 mai întâi se determină drepturile efective ale utilizatorului în directorul părinte - DIR1 în acest exemplu. În funcţie de masca drepturilor moştenite (IRM) pentru SUBDIR1 şi SUBDIR2, se determină drepturile efective.

Observaţie

Dreptul de Supervisory nu poate fi niciodată revocat din mască. Totuşi, în acest caz prezenţa lui în mască nu are nici un efect, deoarece utilizatorului nu i-a fost acordat acest drept prin TA (nu îl poate moşteni dacă nu îl are în directorul părinte).

3. Dacă unui utilizator i-a fost acordat dreptul de Supervisory într-un director, acesta va avea toate drepturile în toate subdirectoarele şi fişierele sale, fără a se ţine seama de existenţa asignărilor "trustee" (TA) pe nivelurile inferioare sau de restricţiile introduse prin IRM.

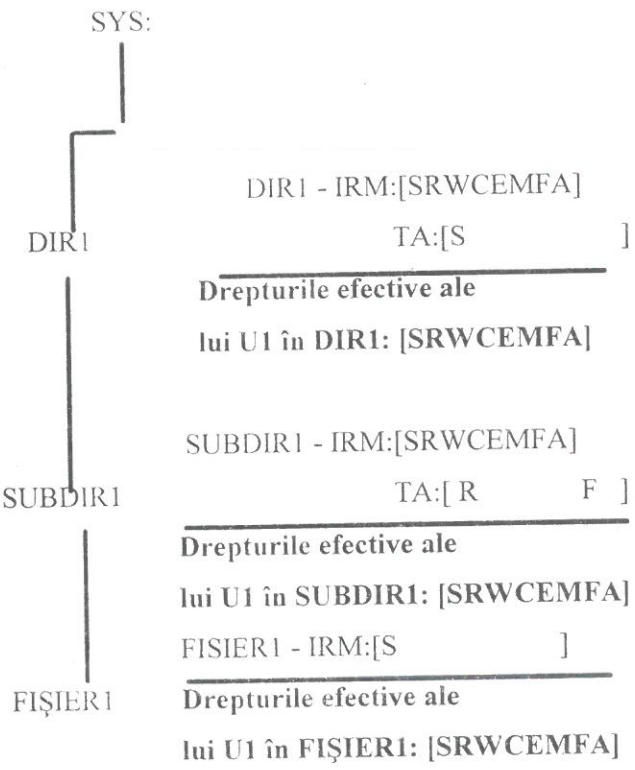
Ştiind că dreptul de Supervisory nu poate fi niciodată revocat din mască, atunci odată acordat în directorul părinte, utilizatorul îl va moşteni în toate subdirectoarele şi fişierele acestuia.

Atributele fişierelor şi directoarelor

Al treilea nivel de securitate este implementat la nivelul directoarelor, respectiv fişierelor, prin specifica-rea atributelor. Atributele sunt caracteristici speciale care se acordă anumitor directoare sau fişiere.

Atributele au întâietate comparativ cu TA, în sensul că pot împiedica realizarea de către utilizator a unor operaţii pe care drepturile efective le permiteau. Astfel, specificarea atributelor poate

împiedica ştergerea unui fişier sau director, copierea unui fişier, modificarea conţinutului unui fişier, vizualizarea numelui unui fişier sau director. De asemenea, atributele se folosesc pentru controlul partajării fişierelor, marcarea fişierelor modificate de la ultima salvare (bitul de arhivare din DOS), protejarea fişierelor împotriva coruperii datelor, intrând sub incidenţa sistemului tranzacţional - TTS (Transactional Tracking System).



Dacă un utilizator are dreptul Modify într-un director sau fişier, el va putea modifica atributele direc-torului, respectiv fişierului şi apoi efectua orice operaţie permisă de drepturile sale efective.

Atributele ce pot fi acordate directoarelor sunt: Delete Inhibit; Hidden: Purge; Rename Inhibit; System .

Atributele ce pot fi acordate fişierelor sunt: Archive Needed; Copy Inhibit; Delete Inhibit; EXecute Only; Hidden: Indexed; Purge; Read Audit; Read Only/Read Write; Rename Inhibit; Shareable; System; Transactional; Write Audit.

Utilitarele NetWare afişează atributele prin iniţialele lor între paranteze drepte:

[Ro S A X H Sy I T P Ra Wa C D R].

Prin convenţie, nespecificarea unui atribut pentru un director sau fişier va fi indicată printr-un blank în locul iniţialei:

[Ro S D R].

Archive Needed (A) poate fi atribuit numai fişierelor. NetWare automat îl atribuie oricărui fişier care e modificat de la ultima salvare prin Backup. Acest atribut este bitul Archive din DOS.

Copy Inhibit (C) poate fi atribuit numai fişierelor. El restricţionează dreptul de copiere a fişierelor nu-mai pentru utilizatorii legaţi la staţii Macintosh. Chiar dacă utilizatorii au dreptul de Read şi File Scan la nivel de director sau fişier, ei nu vor putea copia fişiere. Dacă însă utilizatorii Macintosh au dreptul Modify, ei vor putea anula atributul Copy Inhibit şi apoi copia fişierul.

Delete Inhibit (D) poate fi atribuit directoarelor şi fişierelor. Acest atribut împiedică utilizatorii să ştear-gă directoare sau fişiere chiar dacă aceştia au dreptul Erase acordat la nivel de director sau fişier. Dacă însă utilizatorilor le-a fost acordat dreptul Modify, ei vor putea anula atributul Delete Inhibit şi apoi şterge fişierul sau directorul.

Execute Only (X) poate fi atribuit numai fişierelor. Acest atribut poate fi acordat doar de supervizorul reţelei şi numai fişierelor cu extensia .EXE sau .COM. El va împiedica copierea acestor fişiere, iar odată atribuit nu mai poate fi anulat (este bine a se păstra cópii dupa astfel de fişiere). Utilitarul BACKUP nu va salva astfel de fişiere şi este posibil să nu se execute corect anumite programe atunci când li s-a atribuit Execute Only.

Hidden (H) poate fi atribuit directoarelor şi fişierelor. Acest atribut "ascunde" fişierul sau directorul la introducerea comenzii DOS DIR şi împiedică ştergerea sau copierea acestora. Totuşi fişierul sau directorul vor apare într-o căutare cu comanda de reţea NDIR (numai dacă utilizatorul are dreptul de File Scan).

Indexed (I) poate fi atribuit numai fişierelor. În mod automat, NetWare îl atribuie fişierelor cu peste 64 de intrări în tabela FAT (File Allocation Table). Indexarea duce la creşterea vitezei de acces pentru fişierele mari.

Purge (P) poate fi atribuit directoarelor şi fişierelor. Dacă este atribuit unui fişier, la ştergerea logică a acestuia cu comanda DELETE, sistemul NetWare îl va şterge din evidenţa sa, iar fişierul nu mai poate fi recuperat cu comanda SALVAGE. Când este atribuit unui director, sistemul NetWare va şterge din evidenţă toate fişierele din director în

momentul ştergerii lor, iar acestea nu mai pot fi recuperate cu utilitarul SALVAGE.

Observaţie

Un fişier normal după ce a fost şters, blocurile deţinute de acesta pe disc nu se alocă imediat pentru noile fişiere ce se scriu pe disc (pentru acestea din urmă se alocă zona liberă rămasă pe disc), astfel încât fişierele şterse pot fi recuperate. Cu atributul Purge se va şterge informaţia de recuperare.

Read Audit (Ra) poate fi atribuit numai fişierelor. Acest atribut nu a fost implementat în NetWare v.3.11.

Read Only (Ro) poate fi atribuit numai fişierelor. Când Ro este atribuit unui fişier, NetWare automat îi atribuie Delete Inhibit şi Rename Inhibit. În consecinţă, utilizatorii nu vor putea modifica, şterge sau redenumi fişierul, chiar dacă aveau drepturile Write şi Erase acordate la nivel de fişier sau director. Acest atribut va putea fi anulat de acei utilizatori care au dreptul de Modify în fişier, anulându-se automat şi atributele Delete Inhibit şi Rename Inhibit, astfel încât utilizatorii vor putea modifica, redenumi sau şterge fişierul. Utilizatorii ce au dreptul Modify în fişier pot anula numai atributul Delete Inhibit sau Rename Inhibit, fără a anula şi Read Only, astfel încât ei pot şterge sau redenumi fişierul, dar fără a scrie în el. Când atributul Read Only nu este setat, fişierele sunt marcate cu Read Write, (Rw), care reprezintă setarea implicită.

Rename Inhibit (R) poate fi atribuit directoarelor şi fişierelor. Acest atribut împiedică utilizatorii să redenumească directoare şi fişiere, chiar dacă aceştia aveau acordat dreptul Modify la nivel de director, respectiv de fişier. Dacă însă utilizatorii au dreptul Modify, ei pot anula atributul Rename Inhibit şi apoi să redenumească fişierul sau directorul.

Shareable (S) poate fi atribuit numai fişierelor. Acest atribut permite accesul simultan al mai multor utilizatori la fişierul respectiv, acesta devenind fişier partajabil. El este utilizat de regulă împreună cu atributul Read Only.

Observaţie

Pentru ca un program să poată fi partajat, nu este suficient să i se atribuie Shareable, programul însuşi trebuie să aibă capacitatea de lucru în regim "multi-user".

System (Sy) poate fi atribuit fişierelor şi directoarelor. Directorul, respectiv fişierul, va conţine informa-ţia de sistem. Acest atribut va "ascunde" fişierul sau directorul la o introducere a comenzii DOS DIR şi va împiedica ştergerea sau copierea lor. Totuşi fişierul sau directorul vor apare într-o căutare cu comanda NetWare NDIR, dacă utilizatorul are dreptul de File Scan.

Transactional (T) poate fi atribuit numai fişierelor. Un fişier marcat cu acest atribut va intra în evidenţa sistemului tranzacţional (Transactional Tracking System - TTS). TTS împiedică coruperea datelor, asigurând în momentul actualizării unui fişier ori că toate modificările s-au efectuat, ori că nici una nu se va efectua. Toate fişierele de baze de date ce se doresc a fi protejate împotriva coruperii datelor vor trebui marcate cu acest atribut.

Write Audit (Wa) poate fi atribuit numai fişierelor. Acest atribut nu a fost implementat în NetWare v. 3.11.

Pentru a vizualiza sau modifica atributele fişierelor se utilizează: FLAG sau FILER.

Pentru a vizualiza sau modifica atributele directoarelor se utilizează: FILER sau FLAGDIR.

Securitatea la file server

Al patrulea nivel de securitate este securitatea la file server. Consola file serverului este monitorul şi tas-tatura de la care se poate vedea şi controla activitatea serverului. De la consola file serverului se pot introduce comenzi pentru controlul imprimantelor şi driverelor de disc, se pot trimite mesaje, se poate seta ceasul file serverului, se poate opri file serverul sau se poate vizualiza informaţia cu privire la server. Orice intrare neautorizată la reţea de la consola file serverului poate avea efecte dezastruoase. Se poate preveni accesul neautorizat la consola file serverului în două moduri:

- să se folosească facilitatea de blocare a tastaturii până la tipărirea parolei supervizorului sau a parolei consolei (cea dată la blocare). Această opţiune este disponibilă după încărcarea modulului MONITOR;
- să se folosească comanda SECURE CONSOLE pentru a nu permite încărcarea modulelor din partiţia DOS, de pe o dischetă sau din orice alt director din NetWare în afară de SYS:SYSTEM, a nu permite altui utilizator în afara operatorului consolă să schimbe data şi timpul, iar SO DOS să nu mai poată fi accesat de la consola file serverului.

5. Mapări de drivere sub NetWare

Accesul pe directoare

Asemenea sistemului de operare MS-DOS, NetWare foloseşte literele alfabetului pentru a reprezenta diferite locaţii de stocare a datelor sau drivere.

În cazul sistemului de operare MS-DOS, driverul A este asociat primei unităţi interne de disc flexibil, iar driverul B celei de-a doua (dacă ea există). Depinzând de tipul staţiei de lucru, driverul C poate fi asociat hard discului acesteia.

Observaţii

1. Litera B este automat folosită chiar dacă nu există a doua unitate fizică de disc flexibil. În acest mod, un calculator cu o singură unitate fizică de disc flexibil, are două unităţi logice de disc flexibil (driverele A şi B).
2. Dacă hard discul este partiţionat, atunci litera C va reprezenta partiţia primară, iar următoarele li-tere (D, E şamd.) vor reprezenta driverele logice, emulate pe partiţia extinsă (vezi comanda DOS **FDISK.EXE**).

Spre deosebire de driverele locale, ce sunt asociate unităţilor fizice de disc ale staţiei de lucru, driverele de reţea sunt asociate unor locaţii particulare din structura de directoare a file serverului. Astfel, procesul de mapare va reprezenta atribuirea unei căi director unui driver de reţea. Se pot utiliza 26 litere (de la A la Z) drept identificatori de drivere ("pointeri").

NetWare recunoaşte trei tipuri de drivere: locale, de reţea, de căutare.

Drivere locale

Driverele locale sunt asociate unităţilor fizice de disc, instalate pe staţia de lucru (ele pot fi: unităţi de disc flexibil sau unităţi de disc hard). În mod implicit, NetWare presupune că primele litere din alfabet (de la A la E) reprezintă driverele locale ale staţiei.

Observaţie

Dacă utilizatorul doreşte să schimbe numărul de drivere locale, va introduce comanda LASTDRIVE în fişierul de configurare al sistemului de operare local al staţiei (CONFIG.SYS). Rolul comenzii LASTDRIVE este de a fixa numărul maxim de drivere logice la care sistemul de operare MS-DOS are acces (LASTDRIVE=x, unde x poate fi orice literă de la A la Z, iar valoarea sa va reprezenta ultimul driver pe care sistemul de operare MS-DOS îl va accepta).

Implicit, la încărcarea sa, sistemul de operare MS-DOS presupune că există cel puţin 5 drivere instalate (A-E). După cum se poate observa, comanda LASTDRIVE îşi găseşte utilitatea numai într-o reţea.

Drivere de reţea

Driverele de reţea permit utilizatorului accesul direct la o locaţie particulară în cadrul structurii de directoare a file serverului. Pentru a mapa un driver de reţea pe un anumit director, se foloseşte comanda MAP (comandă NetWare). În mod implicit, NetWare consideră că primul driver de reţea este F.

Drivere de căutare

Driverele de căutare permit utilizatorului să execute fişiere program, localizate într-un alt director decât cel curent.

Observaţie

Efectul mapării unui driver de căutare este similar cu cel al comenzilor PATH şi APPEND (din DOS).

Driverele de căutare sunt numerotate (deşi, acestea sunt, de asemenea, reprezentate şi prin litere). În cazul unui driver de căutare, identificatorul de driver este ales începând cu litera nealocată cea mai îndepărtată. Astfel, în mod implicit, primul driver de căutare (SEARCH1 sau S1) va fi driverul Z, al doilea (SEARCH2 sau S2) va fi Y, şamd, în ordine alfabetică inversă. Dacă utilizatorul specifică de la linia de comandă numele unui fişier executabil, fără a-i preceda un nume de cale, NetWare execută căutarea acestuia în următoarea ordine:

1. în directorul curent;
2. în directoarele pe care s-au mapat drivere de căutare şi anume în ordinea numerotării acestora (fişierul executabil este căutat mai întîi în driverul S1, apoi în S2, şamd).

Observaţie

Sistemul de operare NetWare permite fiecărui utilizator să aibă 16 drivere de căutare din totalul de 26 drivere disponibile pentru fiecare staţie.

Mapări de drivere (comanda MAP)

Se utilizează comanda **MAP** pentru a realiza următoarele operaţii:

- afişarea mapărilor curente: **MAP** [identificator_de_driver]
- maparea unui driver de reţea pe directorul specificat: **MAP** identificator_driver = cale_director

- maparea unui driver de căutare pe directorul specificat: **MAP** id_driver_de_căutare = cale_director
- inserarea unui nou driver de căutare: **MAP INS[ERT]** id_driver_de_căutare = cale_director
- ştergerea unui driver de reţea sau de căutare: **MAP DEL[ETE]** identificator_driver

6. Login Script

Login Script (LS) reprezintă un set de comenzi pe care sistemul le execută ca parte a procedurii de co-nectare la reţea. Comenzile conţinute în LS vor iniţializa mediul de lucru pentru utilizatorul ce a căpătat acces la resursele file serverului (acestea fiind comenzi pentru iniţializarea variabilelor de mediu, mapări de drivere de reţea, mapări de drivere de căutare, afişarea mesajelor şi comenzi de control al execuţiei programelor utilizatorului).

După ce utilizatorul a iniţiat cererea de conectare la file server (comanda LOGIN) şi a introdus corect numele şi parola, programul LOGIN.EXE va executa setul de comenzi din LS. NetWare utilizează trei tipuri de LS:

LS de sistem, LS individual, LS implicit.

Login Scriptul de sistem

Permite supervizorului să seteze mapări generale de drivere de reţea şi de căutare pentru toţi utilizatorii. De asemenea, el include comenzi ce vor fi executate pentru toti utilizatorii sau numai pentru grupuri definite de utilizatori. LS de sistem este creat de către supervizorul reţelei în cadrul utilitarului SYSCON (opţ. *Supervisor Options*) şi este salvat în fişierul NETSLOG.DAT din directorul SYS:PUBLIC.

Observaţie

Deoarece fişierul este stocat într-un director în care toţi utilizatorii au drepturile Read si File Scan, nu este indicată includerea unor parole sau informaţii particulare în login scriptul de sistem.

Login Scriptul individual

Setează variabilele de mediu şi mapările de drivere necesare numai uti-lizatorului respectiv. LS individual poate fi creat şi modificat atât de supervizorul reţelei, cât şi de utilizator. El este conţinut în fişierul cu numele LOGIN (a nu se confunda cu fişierul executabil LOGIN.EXE) şi este localizat în acel subdirector din SYS:MAIL ce are acelaşi nume cu ID-ul (identificatorul) utilizatorului.

Observaţie

Sistemul creează un LS individual vid pentru fiecare utilizator definit pe file server.

Login Scriptul implicit setează mapările de bază pentru sistem:

- mapează primul driver de reţea pe directorul propriu de lucru al utilizatorului SYS:%LOGIN_NAME; iar dacă utilizatorul conectat este supervizorul reţelei îl mapează pe SYS:SYSTEM).

- sunt definite două drivere de căutare, primul mapat pe SYS:PUBLIC şi respectiv, al doilea mapat pe directorul ce conţine fişierele sistemului de operare local al staţiei (MSDOS).

El conţine următoarele comenzi:

WRITE "Good %GREETING_TIME, %LOGIN_NAME."

MAP DISPLAY OFF

MAP ERRORS OFF

Rem: Set 1st drive to most appropiate directory.

MAP *1:=SYS:;*1:=SYS:%LOGIN_NAME

If "%1"="SUPERVISOR" THEN MAP *1:=SYS:SYSTEM

Rem: Set search drives (S2 machine-OS dependent).

MAP INS S1:=SYS:PUBLIC

MAP INS S2:=S1:%MACHINE /%OS/ %OS_VERSION

Rem: Now display all the current settings.

MAP DISPLAY ON

MAP

Observaţie

LS implicit nu poate fi editat, fiind conţinut în fişierul executabil LOGIN.EXE, din SYS:LOGIN şi SYS:PUBLIC.

La conectarea la file server, numai unul sau două din LS menţionate pot fi executate, dar niciodată toate trei. Ordinea de execuţie este următoarea:

1. Dacă există, LS de sistem se va executa primul.
2. Al doilea se va executa LS individual, dacă nu este vid.
3. LS implicit se execută dacă LS individual nu există sau este vid, indiferent dacă LS de sistem există sau nu.

Observație

Pentru a executa numai LS de sistem, există două posibilități:

1. Se introduce comanda EXIT la sfârșitul LS de sistem, ceea ce va determina încheierea procedurii LOGIN înaintea verificării existenței LS individual. În acest caz, nici un LS individual nu se mai execută. De asemenea, nu se va mai executa nici LS implicit, pentru acei utilizatori al căror LS individual este vid.
2. Se utilizează comanda LOGIN cu opțiunea "/script", iar LS specificat în comandă va fi fișierul NET$LOG.DAT: **LOGIN /S SYS:PUBLIC\NETSLOG.DAT**

Comenzi ce pot fi utilizate în Login Script

Fișierul LS poate conține diferite tipuri de comenzi:

1. Utilitare NetWare (MAP, ATTACH);
2. Comenzi DOS (se poate seta ambientul DOS din LS, cu ajutorul comenzilor: DOS BREAK, DOS SET, DOS VERIFY);
3. Instrucțiuni de salt:
   - necondiționat (GOTO);
   - condiționat (IF...THEN...ELSE);

Comanda IF...THEN...ELSE este similară comenzilor condiționale din limbajele de programare. (Se pot imbrica până la 10 structuri IF...THEN... ELSE). În cadrul structurilor condiționale din LS putem utiliza:

- variabile identificator, (ce conțin informația curentă despre utilizatorul conectat la file server, cum ar fi data, ora, numele de conectare, numărul stației, numărul conexiunii, ș.a.m.d).

- parametrii formali, care vor fi înlocuiți cu parametrii efectivi specificați în linia de comandă LOGIN.

- variabilele mediului MSDOS (alocate cu comanda DOS SET).

4. Comenzi ce transferă controlul din LS la linia de comandă:
   - # (EXTERNAL PROGRAM EXECUTION) urmată de numele unui fișier executabil. După execuția programului extern se redă controlul următoarei comenzi din LS.
   - EXIT (ce termină execuția LS) urmată de numele unui fișier.EXE, .COM sau BAT, introdus între ghilimele. Astfel comanda EXIT poate transfera o comandă procesorului de comenzi al sistemului de operare local al stației (COMMAND.COM).
5. Comenzi pentru afișarea de texte (WRITE, [F]DISPLAY);
6. Comenzi pentru inserarea de comentarii în LS (REM sau * sau ;).

Observație

Mapările definite de la linia de comandă sunt temporare, în sensul că driverul respectiv va rămâne mapat până când utilizatorul execută LOGOUT sau închide stația de lucru. Dacă însă utilizatorul dorește mapări permanente de drivere de rețea sau de căutare va include comanda MAP în LS. Astfel, comanda MAP este cea mai importantă comandă utilizată în LS.

Login scriptul de sistem

LS de sistem inițializează mediul de lucru pentru toți utilizatorii ce au căpătat acces la resursele file serverului. Principiul de bază în planificarea sa este acela că LS de sistem trebuie să includă cât mai multe comenzi posibile pentru ca LS individuale să fie mai scurte. Anumite comenzi sunt esențiale într-un LS de sistem, unele recomandate, iar altele sunt opționale sau dependente de necesitățile apărute în rețea.

Comenzile esențiale într-un LS de sistem sunt cele care asigură accesul la NetWare și sistemul de operare local al stației. Astfel:

- Pentru a permite accesul utilizatorului din orice director la utilitarele NetWare se mapează primul driver de căutare pe directorul SYS:PUBLIC. **MAP S1:=SYS:PUBLIC**
- Pentru a face posibil accesul utilizatorului din orice director la comenzile sistemului de operare local al stației se mapează al doilea driver de căutare pe directorul MSDOS.

  MAP S2:=SYS:PUBLIC/%OS sau **MAP S2:=SYS:PUBLIC/MSDOS**
- COMSPEC - Comanda asigură reâncărcarea corectă în RAM-ul fiecărei stații de lucru a modulului tranzitoriu al procesorului de comenzi, când s-a încheiat execuția unei aplicații. Comanda trebuie să specifice driverul de căutare, mapat pe directorul MSDOS (în acest caz SEARCH2).

  COMSPEC=S2:COMMAND.COM

Comenzile recomandate într-un LS de sistem fac posibil accesul la anumite directoare utilizate frecvent:

- Pentru ca utilizatorii să știe în orice moment unde se găsesc în structura de directoare, se recomandă ca prompterul să afișeze în permanență directorul curent.

  Ex. DOS SET PROMPT = "PG"

- Dacă o aplicație este utilizată frecvent de către toți utilizatorii, se mapează următorul driver de căutare (în ordine numerică) pe directorul corespunzător.

  Ex. MAP S3:=SYS:APPS\WORDPROC

- Dacă au fost create grupuri de utilizatori în funcție de aplicațiile utilizate de către aceștia, se pot mapa drivere de căutare numai pentru membrii grupurilor respective, utilizând comanda condițională IF.

```
Ex. IF MEMBER OF "DATABASE"
        THEN
        MAP INS S16 :=SYS:APPS
        \DB
    END
    IF MEMBER OF "WPUSERS"
        THEN
        MAP INS S16 :=SYS:APPS
        \WP
    END
```

- Maparea unui driver de rețea (de obicei primul driver de rețea) pe directorul propriu de lucru al utilizatorului.

```
MAP F := SYS:%
LOGIN_NAME
```

Se poate utiliza și o mapare de driver generic, pentru a mapa primul driver de rețea, fără a specifică litera driverului.

```
MAP *1 := SYS:
%LOGIN_NAME
```

Comenzi opționale

- Afișarea mesajelor pe parcursul execuției LS. Se poate folosi comanda WRITE pentru afișarea unor scurte mesaje.

- Ex: WRITE "GOOD %GREETING_TIME,%FULL_NAME!"

- De asemenea se poate utiliza comanda [F]DISPLAY pentru a afișa mesaje mai lungi, salvate în fișiere de tip text.

```
Ex.: IF MEMBER OF "APPL" THEN
        DISPLAY SYS:APLIC.TXT
    END
```

Observație

Dacă fișierele de tip text specificate în comandă conțin secvențe "Escape", se va folosi comanda DISPLAY.

- Se va utiliza comanda PAUSE după comenzile ce au generat mesaje. Astfel utilizatorii vor avea timp suficient (până la apăsarea unei taste) pentru citirea mesajelor.

- Comenzi pentru atașarea la servere adiționale.

```
Ex.: IF MEMBER OF "ACCT6" THEN
        ATTACH ACCOUNT
        MAP H := ACCOUNT\SYS:
        %LOGIN_NAME
        END
```

7. Exemplu de Login Script de sistem

```
    REM Acesta este un exemplu de LS de sistem
MAP DISLPAY OFF
IF "%ACCESS_SERVER" EQUALS "0" THEN
    WRITE "GOOD %GREETING_TIME,USER
%LOGIN_NAME"
        WRITE
    WRITE "TE-AI CONECTAT LA FILE
SERVER-UL :%FILE_SERVER"
    WRITE "DE LA STATIA %STATION,CU
ADRESA %P_STATION"
    WRITE "SISTEMUL DE OPERARE LOCAL
AL STATIEI ESTE:%OS,%OS_VERSION"
    PAUSE
END
DOS SET PROMPT ="$P$G"
MAP S1:=SYS:PUBLIC
MAP S2:=SYS:PUBLIC\%OS
COMSPEC=S2:COMMAND.COM
        MAP
S3:=SYS:PUBLIC\APPLIC\WORDPROC
        IF NOT MEMBER OF "PART" THEN
    #COMMAND /C BATCH.BAT
END
IF LOGIN_NAME ="SUPERVISOR" THEN
    MAP *1:=SYS:SYSTEM
    MAP *2:=SYS:HOME\SUPERV
ELSE
    MAP *1:=SYS:HOME\%LOGIN_NAME
```

```
END
IF MEMBER OF "DATABASE" THEN
   MAP INS S16:=SYS:APPLIC\DB
END
IF MEMBER OF "WPUSERS" THEN
   MAP INS S16:=SYS:APPLIC\WP
      END
IF MEMBER OF "APPL" THEN
   ATTACH SERVER2
   MAP INS S16:=SERVER2\SYS:APPLIC
   MAP *3:=SERVER2\SYS:%LOGIN_NAME
      END
IF MEMBER OF "WPUSERS" THEN
   #CAPTURE Q=WP_LASER NFF TI=10
ELSE
   IF MEMBER OF "DATABASE" THEN
    #CAPTURE Q=DB_LASER TI=8
   ELSE
    IF MEMBER OF "APPL" THEN
     #CAPTURE S=SERVER2 Q=APL_LASER
TI=20
    END
   END
END
#COMMAND /C CLS
MAP DISPLAY ON
MAP
```

8. Boot-up (Încărcarea)

Încărcarea stației înseamnă alimentarea computerului, încărcarea sistemului de operare local și apoi încăr-carea shell-ului stației. Aceasta se realizează ori cu o dischetă de boot, ori fișierele de boot se pun pe discul hard al stației de lucru.

Crearea dischetei de BOOT

Se inserează discheta în driverul A și se efectuează următoarele operații:

1. se formatează discheta și se transferă sistemul de operare MS-DOS pe dischetă;
2. se copiază fișierele IPX.COM și NETx.COM pe discheta de boot;
3. se copiază fișierele de boot adiționale. Supervizorul de rețea va putea asigura următoarele fișiere:

AUTOEXEC.BAT; CONFIG.SYS; SHELL.CFG.

Crearea fișierului AUTOEXEC.BAT

Se știe că fișierul AUTOEXEC.BAT este un fișier opțional al unui disc sistem, ale cărui comenzi vor fi executate automat după încărcarea sistemului de operare. În cazul nostru este necesar să creăm un fișier AUTOEXEC.BAT care să încarce automat shell-ul stației și protocolul de comunicație. Fișierul mai poate conține comenzi pentru setarea stației pe primul driver de rețea (F) și conectarea utilizatorului la file server (cu comanda LOGIN). De asemenea, se poate seta prompterul DOS astfel încât să indice directorul curent (comanda PROMPT PG).

PROMPT PG <ENTER>

IPX <ENTER>

NET6 <ENTER>

F: <ENTER>

LOGIN servername/username <ENTER>

Observație

Dacă stațiile nu au hard disc și au o singură unitate fizică de disc flexibil (căreia îi sunt asociate două unități logice A și B), atunci este convenabil să disponibilizăm driverele C - E (ce erau locale) pentru driverele de rețea. Pentru aceasta este necesar ca în fișierul CONFIG.SYS să dăm comanda LASTDRIVE=B, ce va seta driverul B ca fiind ultimul driver pe care MS-DOS îl acceptă. Astfel, în fișierul AUTOEXEC.BAT putem seta stația pe driverul C. Se poate seta stația tot pe driverul F, dar ținând seama că utilizatorul are acum încă trei drivere disponibile pentru driverele de rețea (C - E).

Bibliografie

1. **Novell, Inc.**: Novell NetWare Version 3.11 CONCEPTS, 1991.

2. **Novell, Inc.**: Novell NetWare Version 3.11 UTILITIES REFERENCE, 1991.

3. **Novell, Inc.**: Novell NetWare Version 3.11 SYSTEM ADMINISTRATION, 1991.

4. **Novell, Inc.**: Novell NetWare Version 3.11 INSTALLATION, 1991.

5. **Novell, Inc.**: Novell NetWare Version 3.11 SYSTEM MESSAGES, 1991.

6. **Novell Education**: NetWare Version 3.11 SYSTEM MANAGER, 1992.

7. **Novell Education**: NetWare Version 3.11 OS Features Review, 1992.