ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1992
Seria: INFORMATYKA z. 16 Nr kol. 1140

Bożena JURASZCZYK

SIECIOWY SYSTEM OPERACYJNY NETWARE - ORGANIZACJA SIECI I SYSTEM OCHRONY ZASOBÓW (*artykuł przeglądowy*)

Streszczenie. Niniejsze opracowanie zawiera ogólną charakterystykę sieci pracującej w systemie operacyjnym NetWare. Przedstawiono również logiczną organizację zasobów programowych sieci oraz zasady dostępu użytkowników do zasobów sieciowch, jak również opis mechanizmów ochrony tych zasobów przed niepowołanym dostępem.

Summary. This article contents general characteristic of the net which works in operating system NetWare. It contents logic organization of programing storage of the net and user's rules of access to storage and description mechanisms of the protection this storage from undesirable access.

Резюме. Эта разработка включает общую характеристику сети работающей в операционной системе НетВаре. Представлена также логическая организация ресурсов сети, а также принципы доступа пользователей к сетевым ресурсам и описание механизмов защиты этих ресурсов от нежелательного доступа.

1. WPROWADZENIE

Sieciowy system operacyjny NetWare firmy Novell, szczególnie jego wersja ADVANCED NetWare 2.0a, jest bardzo popularny na naszym rynku komputerowym. Nowsze wersje tego systemu są jedynie rozszerzeniem wersji 2.0a o nowe środki programowe.

NetWare jest systemem dzielonych zasobów, to znaczy systemem, w którym jądro systemu funkcjonuje na wyróżnionych stanowiskach sieci - serwerach, zaś fragment systemu, zwany powłoką, pracuje na stanowisku roboczym.

Serwery to stanowiska sieci pełniące specjalizowane funkcje usługowe wobec użytkowników sieci. Można wyróżnić następujące rodzaje serwerów:

- serwery drukarek, które mogą obsługiwać 5 drukarek (3 przez port równoległy Centronics oraz 2 przez port szeregowy RS 232) dostępnych dla wszystkich użytkowników sieci;
- serwery komunikacyjne;
- serwery plików.

Serwer komunikacyjny może pełnić następujące funkcje:

- kontrolę współpracy kilku serwerów pracujących jednocześnie w sieci,
- obsługę, przez jeden serwer, kilku podsieci komunikacyjnych. Jest to tzw. most wewnętrzny (Internal Bridge). W serwerze mogą być zainstalowane cztery pakiety sieciowe dla jednoczesnej obsługi czterech podsieci komunikacjnych (różnych typów).

Internal Bridge integruje podsieci tak, że użytkownicy podsieci "widzą" siebie wzajemnie jak użytkownicy jednej sieci. Praktycznie Internal Bridge pozwala na zwielokrotnienie zasięgu sieci o niewielkim zasięgu pojedynczych podsieci komunikacyjnych oraz na integrowanie podsieci o różnych parametrach technicznych. Można również uzyskać komunikację ze zdalnymi stanowiskami roboczymi (Remote Workstation) przez jeden lub dwa porty szeregowe serwera (RS 232) instalowane logicznie w miejsce jednej lub dwóch kart sieciowch w serwerze.

Podstawową funkcją serwera w systemie NetWare jest dzielenie zasobów programowych zgromadzonych na dyskach twardych serwera - tzw. dyskach sieciowych. Serwer może obsługiwać dwie stacje dysków wewnętrznych oraz do trzydziestu zewnętrznych. Wyposażenie serwerów w dyski zewnętrzne wymaga łączenia ich przez pakiet DCB (Disc Coprocessor Board) firmy Novell. Jest to bardzo kosztowne i dlatego w kraju bardzo rzadko stosowane.

Dyski sieciowe powinny być dyskami o krótkim czasie dostępu (typ i pojemność dysków zależna od wersji programu instalacyjnego). W kraju są stosowane dyski o pojemności do 180 MB.

Serwer w systemie NetWare może pracować w wersji dedykowanej (pełni wyłącznie funkcję serwera) lub w wersji niededykowanej, w której pełni funcję serwera i funkcję stanowiska roboczego. W wersji niededykowanej serwer ma dwa tryby pracy:

– tryb CONSOLE - dla obsługi zleceń konsolowych serwera,
- tryb DOS - dla pracy jako stanowisko robocze.

Wprawdzie praca stanowiska serwera niededykowanego w trybie DOS nie przerywa jego pracy jako serwera, lecz jednak niektóre programy aplikacyjne realizowane na serwerze mogą zakłócać pracę użytkowników sieci. Dlatego zaleca się stosowanie serwera dedykowanego, a w przypadku niededykowanego ograniczenie jego pracy w trybie DOS zarówno w zakresie czasowym, jak i w zakresie uruchamianych programów.

System w wersji niededykowanej wymaga większej pamięci operacyjnej w stanowisku serwera. Ilość wymaganej pamięci operacyjnej serwera zależy od wielkości sieci i wielkości zasobów dyskowych serwera (ze względu na mechanizmy usprawniające obsługę zasobów dyskowych serwera).

Stanowiska robocze to dowolne mikrokomputery IBM PC. Mogą pracować (wyposażone w system MS-DOS lub PC-DOS) niezależnie od sieci korzystając z własnych zasobów dyskowych. W pracy sieciowej korzystają z zasobów dyskowych serwera i mogą nie być wyposażone w stacje dysków (wtedy pakiet sieciowy stanowiska powinien być wyposażony w pamięć typu EPROM zawierającą program zdalnego ładowania systemu). Ze względów praktycznych zaleca się wyposażenie stanowiska w przynajmniej jedną stację dysków elastycznych.

2. ORGANIZACJA ZASOBÓW PROGRAMOWYCH SIECI

Wszelka komunikacja między stanowiskami roboczymi (przesył komunikatów, poczta elektroniczna) odbywa się za pośrednictwem serwera. Użytkownicy nie mają dostępu do lokalnych zasobów innych stanowisk roboczych. Korzystają jedynie z zasobów stanowiska, przy którym aktualnie pracują i z zasobów serwera (serwerów) sieci.

Logiczna organizacja zasobów dyskowych serwera (podobnie jak w systemie MS-DOS lub PC-DOS), to hierarchiczna struktura kartotek, podkartotek i plików. Szczególną jednostką w tej strukturze jest wolumin, którego kartoteka jest kartoteką główną (root directory).

W sieci wieloserwerowej nadrzędną jednostką jest file serwer, który nie jest jednak elementem struktury plików (nie posiada swojej kartoteki). Dostęp

do zasobów serwera uzyskuje się poprzez dostęp do jednego z woluminów serwera. Każdy serwer w sieci ma niepowtarzalną nazwę, określoną w czasie instalacji systemu. Na każdym dysku sieciowym definiuje się jeden lub więcej woluminów. Wolumin to fizyczna część obszaru dysku sieciowego. Ilość, nazwy i rozmiary woluminów ustala się w czasie instalacji systemu. Minimalny obszar woluminu wynosi 10 MB. Zaleca się, by pokrywał się on z całym obszarem dysku sieciowego. Każdy serwer zawiera wolumin - SYS, specyfikowany następująco:

FS1/SYS:

gdzie FS1 jest przykładową nazwą serwera.

W każdym woluminie może być określona jedna lub więcej kartotek. Ilość kartotek w woluminie ustalana jest w trakcie instalacji systemu (organizacja kartotek - dowolna). Każdy użytkownik posiada kartotekę prywatną (home directory), do niej uzyskuje dostęp w chwili włączenia do pracy w serwerze - jest to ochrona przed "zaśmieceniem" publicznych kartotek serwera oraz ochrona prywatnych zasobów użytkownika przed niepowołanym dostępem. Nazwa prywatnej kartoteki użytkownika powinna być identyczna z nazwą użytkownika.

3. SYSTEM OCHRONY ZASOBÓW

Na system ochrony zasobów serwera składa się:

1) ochrona przez nazwę i hasło,
2) ochrona przez prawa powiernicze,
3) ochrona kartotek,
4) ochrona plików przez atrybuty.

W sieci wieloserwerowej każdy serwer ma swój własny system ochrony zasobów niezależny od pozostałych serwerów sieci. W czasie instalacji systemu w serwerze występuje automatyczna rejestracja dwóch użytkowników: SUPERVISOR (administrator) i GUEST (gość). SUPERVISOR przejmuje dalszą kontrolę nad pracą serwera, rejestruje kolejnych użytkowników przez nadanie im nazwy, hasła i praw dostępu do zasobów serwera, kasuje użytkowników (może skasować nawet użytkownika GUEST - co bywa celowe, gdyż pod taką nazwą może się włączyć do

pracy w serwerze zupełnie przypadkowa osoba). Zwykle jednak GUEST nie zostaje skasowany, bo mogłoby to doprowadzić do utrudnienia w pracy innych użytkowników, a przydziela się mu bardzo ubogie prawa.

Dostęp do zasobów serwera uzyskuje się po wprowadzeniu następującej sekwencji:

LOGIN FS1/UZ1

Jeżeli użytkownik UZ1 jest zarejestrowany bez hasła, to następuje włączenie do pracy w systemie. W przeciwnym przypadku pojawia się polecenie wpisania hasła. Polecenie to pojawia się nawet wtedy, gdy nie ma użytkownika, o podanej nazwie - uniemożliwia to wywnioskowanie, czy zła jest nazwa użytkownika, czy hasło, czy też jedno i drugie.

Aby podłączyć się jednocześnie do kilku serwerów, należy po zleceniu LOGIN podać zlecenie ATTACH, co spowoduje przyłączenie następnego serwera. W tym celu można wykorzystać nazwę dowolnego użytkownika, zarejestrowanego w innym serwerze (np.GUEST). Na ogół jednak korzysta się z własnej nazwy, która (jak i hasło), nie musi być identyczna na wszystkich serwerach, na których użytkownik jest zarejestrowany.

W serwerze są rejestrowane również grupy (w trakcie instalacji systemu automatycznie jest rejestrowana grupa EVERYONE). SUPERVISOR może utworzyć nowe grupy. Każdy nowo rejestrowany użytkownik może być włączony przez SUPERVISORA do dowolnej z grup.

Ogólnie można powiedzieć, że prawa dostępu do kartotek lub zbiorów - tzw. prawa efektywne (jeżeli są traktowane jako pewien zbiór praw), są koniunkcją zbioru praw powierniczych i zbioru praw kartoteki. Wśród praw powierniczych użytkownika można wróżnić:

- prawa indywidualne,
- prawa grupowe,
- równoważność praw,

co zostanie bardziej szczegółowo omówione w dalszej części niniejszego opracowania.

Każdy typ praw oznacza możliwość korzystania z kombinacji poniższych praw:

R - prawo czytania w otwartym pliku,

W - prawo pisania w otwartym pliku,

O - prawo otwarcia pliku,

C - prawo tworzenia z otwarciem pliku,
D - prawo kasowania pliku,
P - tzw.prawo parentalne (tworzenie, zmiana nazwy i kasowanie podkartoteki, nadawanie praw powierniczych i praw kartoteki w danej kartotece i jej podkartotekach),
S - prawo przeszukiwania kartoteki,
M - prawo modyfikowania atrybutów plików.

Każdemu użytkownikowi mogą być nadane pewne prawa w stosunku do określonej kartoteki - ten rodzaj praw nazywa się właśnie prawami powierniczymi. Upoważnionym do nadawania praw użytkownikowi jest SUPERVISOR i każdy użytkownik mający prawa parentalne w danej kartotece lub w kartotece bezpośrednio nadrzędnej. Użytkownik posiadający prawa powiernicze nazywany jest powiernikiem.

Prawa powiernicze użytkownika w odniesieniu do kartoteki uzyskuje się jako połączenie praw nadanych indywidualnie, grupowych i równoważnych. Zatem prawa indywidualne posiada powiernik kartoteki. Prawa grupowe posiada grupa użytkowników, która jako całość jest powiernikiem danej kartoteki. Równoważność praw polega na tym, że dowolnemu użytkownikowi lub grupie użytkowników można nadać prawa równoważne prawom innego użytkownika lub grupy. Prawa grupowe są więc szczególnym przypadkiem zasady równoważności praw. Można w ten sposób na dać dowolnemu użytkownikowi prawa SUPERVISORA i wówczas ten użytkownik także będzie pełnił rolę administratora w sieci.

Prawa powiernicze użytkownika (lub grupy) określone w pewnej kartotece są dziedziczone na podkartoteki tak długo, aż nie zostaną zmienione na pewnym poziomie.

Prawa kartotek służą do określenia maksymalnych praw, z jakich mogą korzystać powiernicy w danej kartotece. Są one nadawane kartotece w momencie jej tworzenia lub są przyjmowane domyślnie wszystkie (co później może ulec zmianie). Upoważnionym do nadawania praw kartoteki jest SUPERVISOR i każdy użytkownik mający prawa parentalne w danej kartotece lub w bezpośrednio nadrzędnej.

Z powyższych stwierdzeń wynika, że nawet użytkownik posiadający określone prawo powiernicze nie będzie mógł z niego korzystać w kartotece, która nie zawiera tego prawa wśród własnych praw kartoteki. Prawa kartoteki nie są dziedziczone na podkartoteki.

Prawa efektywne użytkownika w określonej kartotece to takie, z których użytkownik może faktycznie korzystać w tej kartotece. Dlatego można powiedzieć, że prawa efektywne są koniunkcją zbioru różnego rodzaju praw powierniczych i zbioru praw kartoteki. SUPERVISOR jest użytkownikiem, który posiada efektywnie wszystkie prawa we wszystkich kartotekach.

Pliki na dyskach sieciowych są opatrzone flagami oznaczającymi ich atrybuty, z których tylko Read-Only/Read-Write bezpośrednio odnosi się do ochrony zasobów na dyskach sieciowych. Ustawiony atrybut Read-Only jest nadrzędny nad efektywnymi prawami dostępu do kartoteki. Dotyczy to nawet SUPERVISORA, który jednak może zmienić ten atrybut. Pozostałe atrybuty mają znaczenie informacyjne lub organizacyjne. Przykładem może być atrybut Shareable/Non-Shareable, który informuje czy dostęp do pliku ma jeden, czy kilku użytkowników.

4. PODSUMOWANIE

System operacyjny NetWare jest przeznaczony dla użytkowniów sieci, zaznajomionych z obsługą komputerów IBM PC i pracą na tych komputerach w systemie MS-DOS lub PC-DOS. Podstawowym zadaniem systemu NetWare jest udostępnienie użytkownikom sieci zasobów serwera, które są wspólne dla wielu użytkowników, głównie dysków i drukarek sieciowych. System ten umożliwia komunikację pomiędzy stanowiskami roboczymi i przesył zbiorów (listów) za pomocą tzw. poczty elektronicznej. Wiąże się z tym konieczność wprowadzania mechanizmów ochrony zasobów, co w systemie NetWare jest rozwiązane w sposób wystarczająco skuteczny i prosty.

LITERATURA

1. NetWare User Reference, Novell Incorporated Orem, Utah. 1986.
2. Sieciowy system operacjny NetWare - materiały dydaktyczne. Pol.Śl.Instytut Informatki, Gliwice 1989.

Recenzent: doc.dr inż. Bolesław Firganek

Wpłynęło do Redakcji: 29.06.1990 r.

NET OPERATING SYSTEM NETWARE - ORGANIZATION OF THE NETS AND PROTECTION SYSTEM OF STORAGE

Abstract

A Local Area NetWare (LAN) links personal computers together so they can communicate and share resources. Novell's NetWare operating system is a high-performance local area network control program designed to provide NetWare users with sophisticated networking capabilities. With NetWare, users can share network resources (such as hard disks, printers, software applications and datafiles) and access any services that the network provides (such as communication with a mainframe system).

A fully functional NetWare network includes file server, workstations, networking hardware, network hard disks, printers, bridges (internal and external) and others. The file server is a microcomputer that serves as the "heart" of a NetWare network. It runs the NetWare operating system software. The NetWare operating system enables the file server to regulate communications between other personal computers attached to it and to manage any shared resources that may be connected. Workstations are the personal computers operated by the network users. Workstations are used much like ordinary, non - networked computers - each work station processes its own files using its own operating system. However, a NetWare "shell" is loaded into each workstation to enable the workstation to communicate with the file server and the other workstations on the network. A file server in a NetWare network must have at least one hard disk, either internal or external. The NetWare operating system can support up to five hard disk channels, each controlled by a hard disk interface board. A file server in a NetWare network can have up to five printers attached to it. These printers can then be shared by all the users logged in to the file server. Bridges connect two or more networks together to form an internetwork. The NetWare operating system supports internal and external bridging. Internal and external bridging takes place in a within file server, while external bridging takes place in a separate computer outside a file server.

Logic organization of programming storage reminds the one used in DOS. Programming storage protection system consists of four kinds of protection:

1. Login/Password Security
2. Trustee Security
3. Directory Security
4. File Attributes Security.

Each user owing his unique password is assigned his own home directory, his own effective rights, i.e. he may be allowed to create, open or delete files in his home directory but not to have those rights in the other directories belonging to other users. There is a special user called the Supervisor who has the special rights of giving and taking back all the other users rights. Apart from the user's rights also the file attributes, which are assigned to files themselves, are to control user's access to the files.