

ABC Samby

wersja 1.4

1. Czym jest Samba ?

W (prawie) każdej sieci komputerowej znajduje się serwer plików. Jego zadanie jest oczywiste a wymagania przed nim stawiane to przede wszystkim duża niezawodność oraz szybkość działania. Wymagania te dyskwalifikują komputery pracujące pod Windows 3.x/95/98/Me w roli serwera plików. Wydawać by się mogło, że użytkownicy skazani zostali na Windows NT/2000 w tej roli. Okazuje się, że dzięki Sambie, także komputer linuxowy może pojawić się w „otoczeniu sieciowym” oraz udostępnić wszystkie zasoby potrzebne do pracy.

Samba to pakiet narzędzi umożliwiających:

- współdzielenie zasobów (plików, drukarek) w sieci,
- świadczenie usług nazewniczych (rozgłoszeniowych i WINS),
- przeglądanie zasobów sieciowych przez klientów Windows,
- wymuszanie uwierzytelniania nazw użytkowników oraz ich haseł.

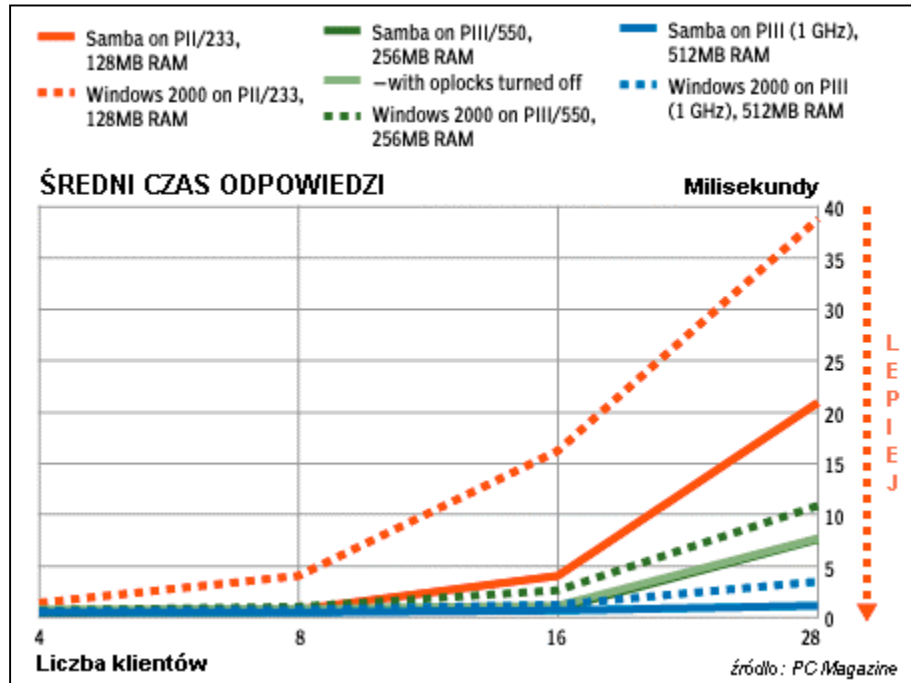
Program ten, dostępny jest za darmo, co znacznie zwiększa jego atrakcyjność. Raz skonfigurowany, działa praktycznie nieprzerwanie (podobnie zresztą jak Linux).

2. Uczeń prześcignął mistrza

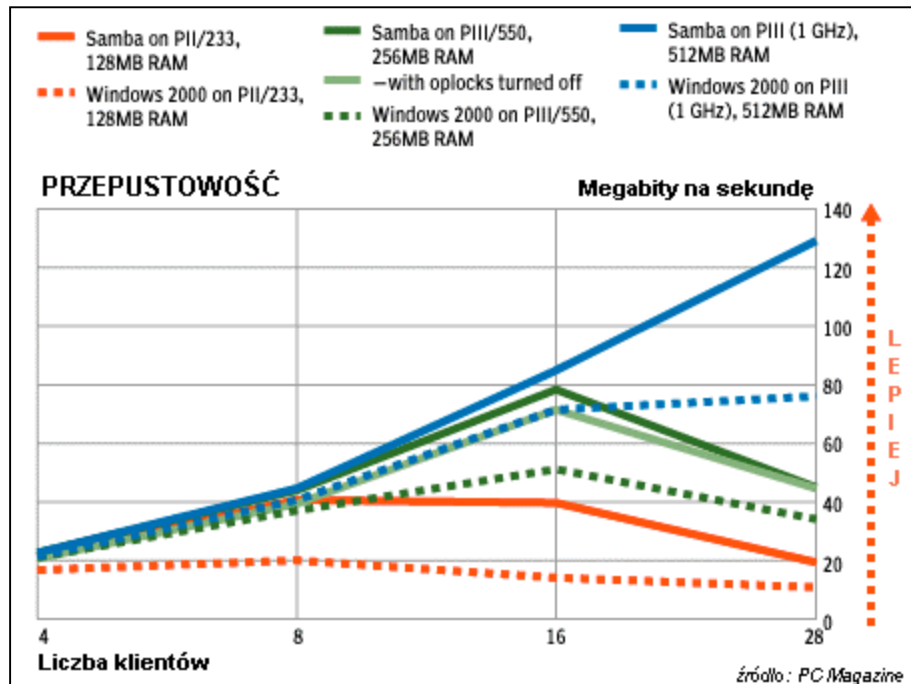
Czytając różnego rodzaju opracowania na temat Samby zauważyłem, że za jej główną zaletę podawano „darmowość”. Można to odczytać w ten sposób: jeśli nie stać Cię na serwer Microsoftu, zainstaluj sobie Linuxa wraz z Sambą. Niewątpliwie ma rację ten, kto uważa, że produkty ww. firmy są drogie. Błędem natomiast jest twierdzenie, że Samba nie ma nic innego do zaoferowania.

Ostatnimi czasy przeprowadzonych zostało wiele testów porównawczych związanych z udostępnianiem plików. Pozwolę sobie zaprezentować tutaj wyniki testów, przeprowadzonych przez PC Magazine (<http://www.pcmag.com>), porównujące wydajność serwerów plików: Windows 2000 oraz Linux + Samba.

Wyniki testów (widoczne na rysunkach poniżej) jednoznacznie wskazują zwycięzcę. Okazuje się bowiem, że zarówno pod względem przepustowości, jak i średniego czasu odpowiedzi (reakcji) serwera, Samba okazała się szybsza. Magazyn IT Week (<http://www.itweek.co.uk>) stwierdza na swoich łamach: „ostatnie wersje Samby przewyższają wydajnością Windows 2000 o około 100%”.



Porównanie wydajności serwerów plików – średni czas odpowiedzi



Porównanie wydajności serwerów plików – przepustowość

3. Pobranie i instalacja Samby

Pierwszym miejscem, do którego należy się udać jest internetowa strona projektu Samba (<http://www.samba.org>) lub jeden z jej mirrorów (np. <http://pl.samba.org>). Witryna ta jest stosunkowo prosta, a nawigacja po niej bardzo intuicyjna. W dziale „downloads” znajduje się ostatnia wersja Samby, jest to plik noszący nazwę samba-latest.tar.gz (gdą powstawała niniejsza praca, ostatnia wersja nosiła numer 2.2.4). Po pobraniu należy wykonać następujące czynności:

- rozpakować ściągnięty plik
tar zxvf samba-latest.tar.gz
- wejść do katalogu zawierającego kod źródłowy programu
cd samba-2.2.4/source/
- przygotować program do kompilacji:
./configure
- skompilować Sambę:
make
- oraz ją zainstalować:
make install

Przed wykonaniem tych czynności, zaleca się zapoznać z informacjami umieszczonymi w katalogu docs. Znajdują się w nich ostatnie informacje dotyczące programu, zmiany, które zostały wprowadzone, dodatkowe opcje wykorzystywane w trakcie kompilacji oraz szczegółowa dokumentacja.

Po wydaniu powyższych poleceń, program zostanie zainstalowany w katalogu /usr/local/samba/. Głównym plikiem konfiguracyjnym Samby jest plik smb.conf. Jest to plik tekstowy, który można edytować dowolnym edytorem. Podzielony jest on na sekcje przez nagłówki, ujęte w nawiasy kwadratowe ([]). Nowy nagłówek sekcji oznacza koniec sekcji poprzedniej. Można także umieszczać w nim komentarze, zaczynając linię od znaku hash (#) lub średnika (;) - znaki te są równoważne. Plik ten powinien znajdować się w katalogu /usr/local/samba/lib/.

Pliki wykonywalne programu znajdują się w katalogu /usr/local/samba/bin/. Aby nie podawać za każdym razem pełnej ścieżki dostępu do nich, proponuję umieścić tą ścieżkę w zmiennej PATH w pliku /etc/profile.

4. Linux w „otoczeniu sieciowym”

Na początek przedstawię konfigurację, dzięki której Linux pojawi się w „otoczeniu sieciowym”. Nie będzie on co prawda nic udostępniał, ale dzięki temu można będzie się przekonać, czy program został skompilowany i zainstalowany poprawnie. Uważam, że jest to dobry sposób, aby rozpocząć pracę ze świeżo zainstalowaną Sambą.

Na początek w pliku smb.conf wystarczy umieścić:

```
[global]
workgroup = Workgroup
netbios name = Pingwin
server string = Serwer linuxowy
security = share
```

Oto opis poszczególnych pozycji:

[global]

zawiera parametry odnoszące się do wszystkich funkcji serwera. Są to parametry modyfikujące zachowanie całej Samby. Jest to jedyna sekcja, która jest potrzebna, aby komputer zaistniał w „otoczeniu sieciowym”.

workgroup

zawiera nazwę grupy roboczej, w której pracują komputery. Tutaj jej nazwa (wartość) to *Workgroup*. Taką samą nazwę grupy roboczej mają komputery pracujące pod Windows. Równie dobrze może być to *Osiedlowa*.

netbios name

definiuje nazwę, pod jaką komputer linuxowy pojawi się w „otoczeniu sieciowym”.

server string

to tekst wyświetlany wraz z nazwą komputera w „otoczeniu sieciowym”, dodatkowa informacja.

security

ustawia zabezpieczanie na poziomie zasobów, co jest najbardziej odpowiednie na potrzeby, które będą definiowane w dalszej części pracy.

Aby ułatwić sobie życie, proponuję utworzyć link symboliczny w katalogu */etc/* do pliku */usr/local/samba/lib/smb.conf*:
`ln -s /usr/local/samba/lib/smb.conf /etc/smb.conf`
Dzięki temu plik konfiguracyjny programu znajdzie się w katalogu, w którym mieszczą się pliki konfiguracyjne innych programów a dostęp do niego będzie ułatwiony dzięki krótszej ścieżce. Aby przetestować składnię pliku konfiguracyjnego Samby, należy posłużyć się poleceniem *testparm*. Jeśli coś jest nie w porządku, zostanie napisany odpowiedni komunikat. Powyższy program zwróci wartości wszystkich pozostałych parametrów programu. Na razie nie należy się nimi przejmować.

5. Uruchomienie Samby

Jak już wspomniałem – Samba to zbiór programów spełniających określone funkcje. Najważniejszymi z nich są dwa demony: programy *smbd* oraz *nmbd*. Demon *smbd* zapewnia klientom dostęp do współdzielonych plików i drukarek. Oprócz tego odpowiada za usługę przeglądania, uwierzytelnianie użytkowników, blokowanie zasobów i współdzielenie danych. Demon *nmbd* to serwer nazw który dodatkowo bierze udział w wyborze przeglądarki.

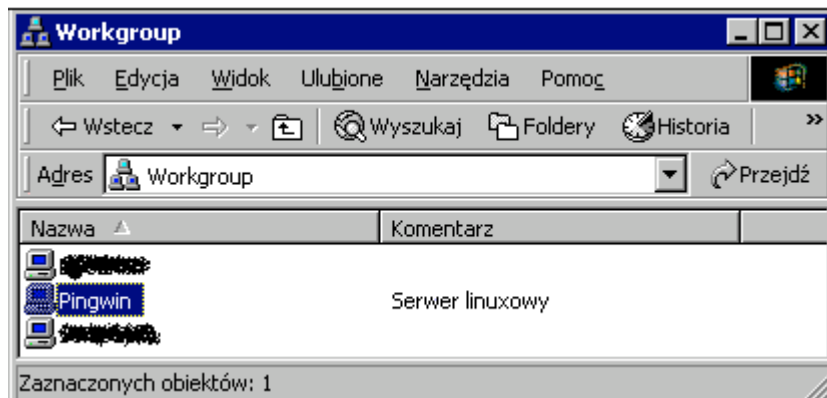
Inne, mniej ważne lecz przydatne programy, zostaną omówione w dalszej części tej pracy. Aby Samba mogła pracować poprawnie, w systemie muszą działać dwa ww. procesy. Zalecany sposób pracy Samby jest uruchomienie ich jako demonów autonomicznych – demonów, które działają w systemie cały czas, niezależnie od tego czy potrzeba taka istnieje, czy nie.

Aby uruchomić Sambę, należy wydać poniższe polecenia, które:

- uruchamiają demona smbd:
/usr/local/samba/bin/smbd -D
- uruchamiają demona nmbd:
/usr/local/samba/bin/nmbd -D

Od tej pory Samba powinna działać. Aby przekonać się, czy tak jest naprawdę, można użyć polecenia: `ps x |grep "mbd -D"`

Wynikiem powinny być zwrócone programy, które przed chwilą zostały uruchomione. Przede wszystkim jednak komputer o nazwie „Pingwin” powinien pojawić się w „otoczeniu sieciowym”:



Komputer linuxowy w „otoczeniu sieciowym”

Teraz można być pewnym, że kompilacja i instalacja serwera przebiegła prawidłowo.

6. Udostępnienie pierwszego zasobu

Kolejnym krokiem, na drodze konfiguracji serwera plików, będzie udostępnienie fragmentu dysku dla wszystkich komputerów. Będzie to zasób, do którego wszyscy użytkownicy posiadający pełny dostęp – a więc prawa zapisu, odczytu oraz prawa do kasowania. Uważam, że zasób taki jest szczególnie przydatny w sieciach domowych, osiedlowych a także w małych firmach. Może to być miejsce trzymania dokumentów firmowych, różnego rodzaju plików do wymiany między użytkownikami itp.

Zasób, który zostanie udostępniony pojawi się w „otoczeniu sieciowym” pod nazwą „poligon”. Najpierw na dysku serwera należy utworzyć katalog i nadać mu prawa zapisu, odczytu oraz uruchamiania dla wszystkich użytkowników:

```
mkdir /mnt/dla_wszystkich  
chmod 0777 /mnt/dla_wszystkich
```

W ten sposób utworzony zostanie katalog (na dysku lokalnym serwera) dla_wszystkich, który pojawi się w „otoczeniu sieciowym” pod nazwą „poligon”. Oczywiście miejsce jego utworzenia na dysku zależy od administratora i może być to zupełnie inne miejsce. Pozostała jeszcze konfiguracja Samby. Należy wyedytować plik smb.conf dopisując do niego:

```
[poligon]
comment = Dysk do wymiany danych
path = /mnt/dla_wszystkich
create mask = 0777
directory mask = 0777
browsable = yes
writable = yes
guest ok = yes
```

Po każdej przeprowadzonej zmianie w tym pliku proponuję wykonać polecenie testparm, aby przekonać się czy składnia pliku jest poprawna.

Oto opis poszczególnych pozycji:

[poligon]

definiuje nową sekcję pliku smb.conf, wyznacza jednocześnie nazwę, pod jaką pojawi się zasób w „otoczeniu sieciowym”.

comment

jak łatwo się domyślić, jest to komentarz dotyczący zasobu. Informacja ta pojawi się w „otoczeniu sieciowym” przy udostępnianym katalogu.

path

jest ścieżką dostępu na lokalnym dysku serwera do udostępnianego zasobu.

create mask

definiuje z jakimi prawami dostępu pojawią się tworzone na dysku pliki. Maska 0777 oznacza prawa pełnego dostępu dla wszystkich. Synonimem jest parametr create mode.

directory mask

określa prawa dostępu ustawiane podczas tworzenia katalogów. Podobnie jak w przypadku plików, prawa pełnego dostępu otrzymuje każdy użytkownik. Synonimem jest parametr directory mode.

browsable

parametr, którego domyślną wartością jest „yes”, określa czy dany zasób ma być widoczny dla klientów. Synonimem jest browseable.

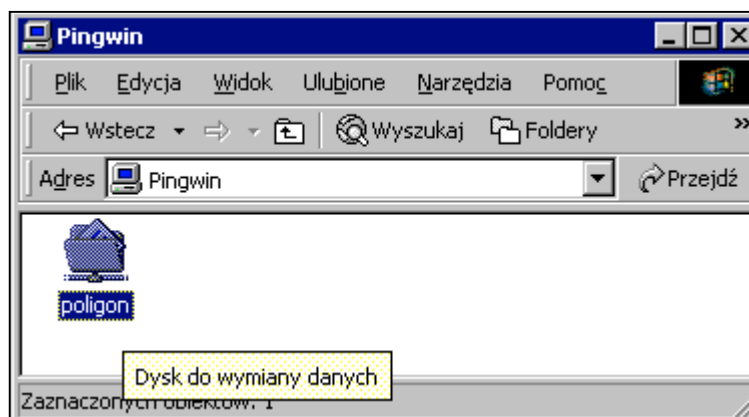
writable

gdy ustawiony na „yes”, użytkownicy mogą tworzyć oraz modyfikować istniejące pliki oraz katalogi. Synonimami są writeable oraz (o przeciwnym znaczeniu) read only.

guest ok

gdy ustawiony na „yes”, parametr ten zapewnia dostęp do zasobu bez konieczności podawania hasła. Synonimem jest public.

W ten sposób utworzony został pierwszy zasób udostępniany przez Sambę. Pozostało tylko wykonać polecenie testparm aby przekonać się, czy w czasie edycji nie popełniono błędu (np. literówki) oraz uruchomić Sambę. Następnie należy sprawdzić, czy faktycznie zasób istnieje w „otoczeniu sieciowym” a następnie przekonać się, czy każdy posiada do niego pełne prawa.



Pierwszy zasób udostępniony przez Sambę

7. Samba a sprawa polska

Czytając grupy dyskusyjne zauważyłem, że stosunkowo często pojawia się pytanie „jak zmusić Sambę do korzystania z polskich literek?”. Faktycznie, wykorzystując powyższą konfigurację użytkownik m.in. Windows 98 napotka „Błąd systemu plików (nr 1026)” próbując np. usunąć plik zawierający w nazwie polskie litery. Aby skorygować ten błąd wystarczą dwa dodatkowe wpisy w pliku smb.conf, w sekcji [global]:

```
character set = ISO8859-2
client code page = 852
```

Komputery pracujące pod Ms Windows używają swojej własnej strony kodującej znaki (polskie definiuje strona kodowa 852). Odpowiada jej międzynarodowa strona kodowa, zestaw znaków ISO 8859-2. W ten sposób znikną problemy związane z polskimi literami przy korzystaniu z Samby.

8. Hasła

Do tej pory nie zachodziła konieczność podawania hasła, przy próbie łączenia się z zasobami udostępnianymi przez Sambę. Hasła mogą być przesyłane przez sieć w postaci zaszyfrowanej lub niezaszyfrowanej. Samba obsługuje algorytmy szyfrowania haseł w sieci Windows – może weryfikować tożsamość w taki sam sposób, jak serwery Microsoftu.

Z szyfrowaniem haseł w przypadku Samby związanych jest kilka niedogodności, o których warto wiedzieć:

- należy utworzyć osobną bazę danych z użytkownikami oraz ich hasłami,
- użytkownicy muszą pamiętać o jedno hasło więcej, co może stać się jeszcze bardziej niebezpieczne, niż hasła przesyłanie drogą niezaszyfrowaną,
- jeśli użytkownicy do łączenia się z serwerem używają takich programów jak ftp czy telnet, a pocztę sprawdzają drogą niezaszyfrowaną (co jest standardem) – szyfrowanie traci sens,
- jeśli w sieci lokalnej znajduje się stosunkowo dużo przełączników sieciowych, istnieje małe prawdopodobieństwo przechwycenia hasła.

W dalszej części pracy opiszę wykorzystanie haseł szyfrowanych, gdyż uważam, że większą część tych niedogodności można pominąć odpowiednią konfiguracją systemu oraz niewielkim nakładem dodatkowej pracy.

Aby skonfigurować Sambę do używania szyfrowanych haseł należy w sekcji [global] pliku smb.conf ustawić dwa parametry:

```
encrypt passwords = yes
smb passwd file = /etc/smbpasswd
```

Pierwszy z nich informuje Sambę, aby korzystała z szyfrowanych haseł. Drugi z nich podaje ścieżkę dostępu do pliku, w którym znajduje się baza danych zawierająca użytkowników oraz ich hasła. Nazwa oraz lokalizacja pliku może być dowolna. Pozostało jeszcze utworzyć konta użytkownikom oraz podać ich hasła dostępu do zasobów. Służy do tego polecenie smbpasswd.

- aby utworzyć wpis dla nowego użytkownika (tutaj: paj) należy użyć polecenia z opcją „-a”:
smbpasswd -a paj
- do tymczasowego zablokowania jego konta służy opcja „-d”:
smbpasswd -d paj
- do odblokowania powyższego, należy użyć „-e”:
smbpasswd -e paj
- aby usunąć użytkownika, należy zastosować „-x”:
smbpasswd -x paj
- aby użytkownik zmienił swoje hasło wystarczy, że wywoła on polecenie bez żadnych parametrów:
smbpasswd

Uwaga: przy pierwszym uruchomieniu program zwróci: „unable to open passwd database”. Nie należy się tym przejmować, ponieważ gdy plik z hasłami nie istnieje, program sam go utworzy. Przy dodawaniu kolejnych użytkowników komunikat ten już się nie pojawi. W dalszej części pracy zakładam, że dla każdego użytkownika próbującego łączyć się z Sambą istnieje wpis w pliku z hasłami.

9. Katalog domowy użytkownika

Każdemu użytkownikowi posiadającemu konto na serwerze można udostępnić jego katalog domowy bez potrzeby definiowania każdego z nich osobno. Umożliwia to dostęp użytkownikom do miejsca na dysku serwera z poziomu Windows. Uważam, że jest to idealne miejsce na przechowywanie kopii zapasowych swoich najważniejszych dokumentów.

Dostępowi do katalogów macierzystych poświęcona jest specjalna sekcja o nazwie [homes]. Aby zamienić powyższe słowa w czyn wystarczy do pliku smb.conf dodać odpowiednią sekcję:

```
[homes]
comment = Katalog domowy uzytkownika
writable = yes
```


Po uruchomieniu tak skonfigurowanej Samby każdy użytkownik istniejący w systemie, mający swój wpis w pliku z hasłami może uzyskać dostęp do swojego katalogu domowego na serwerze.

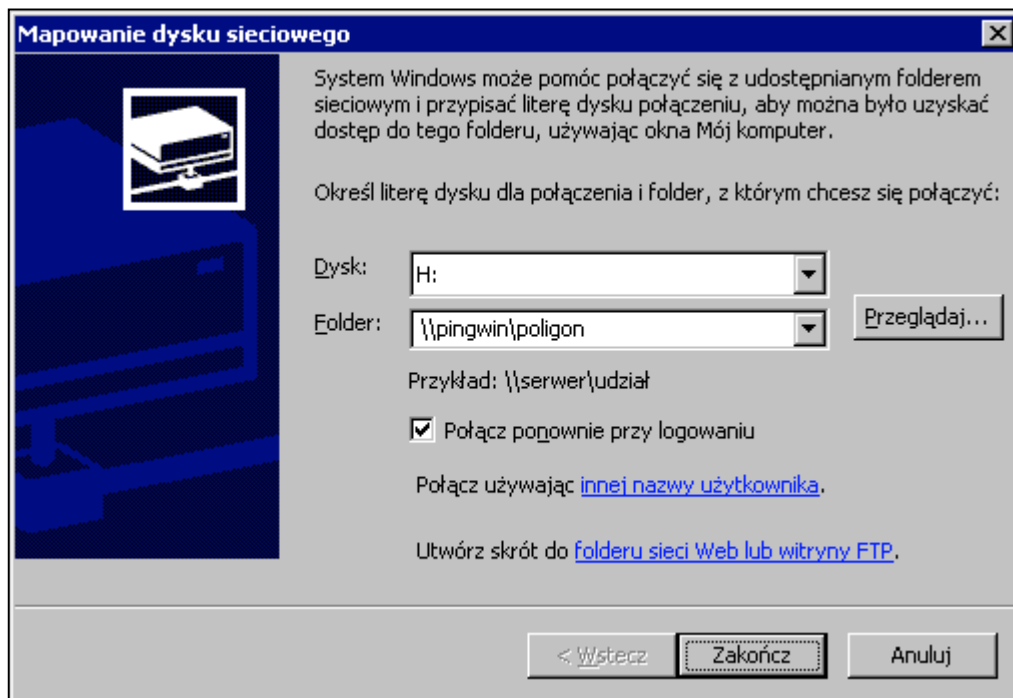
10. Łączenie się z zasobami

Systemy Windows oferują funkcję „mapowania” litery dysku na katalog sieciowy. Dzięki temu aplikacje mogą korzystać z folderu sieciowego, używając standardowej litery dysku.

Windows umożliwia mapowanie dysku na dwa różne sposoby. Pierwszy z nich jest (moim zdaniem) bardziej przyjazny użytkownikowi i odbywa się przy pomocy interfejsu graficznego. Wystarczy z menu „Narzędzia” Eksploratora Windows wybrać „Mapuj dysk sieciowy”. Innym sposobem jest kliknięcie prawym przyciskiem myszki na ikonie „Otoczenie sieciowe” (Win 98/Me) lub „Moje miejsca sieciowe” (Win 2000).

Katalog na zdalnym komputerze jest reprezentowany przez dwa odwrotne ukośniki, po których następuje nazwa zdalnego komputera, kolejny odwrotny ukośnik oraz nazwa sieciowego katalogu (\\zdalny_komputer\katalog). Zapis ten znany jest jako uniwersalna konwencja nazewnicza (Universal Naming Convention, UNC).

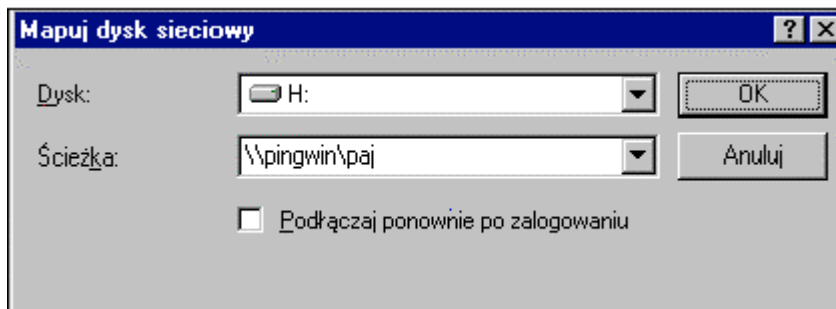
Wykorzystując dotychczasową konfigurację Samby oraz wiadomości przed chwilą poznane spróbuję połączyć się z dyskiem „poligon” (z Windows 2000) oraz z katalogiem domowym użytkownika paj (z Windows 98).



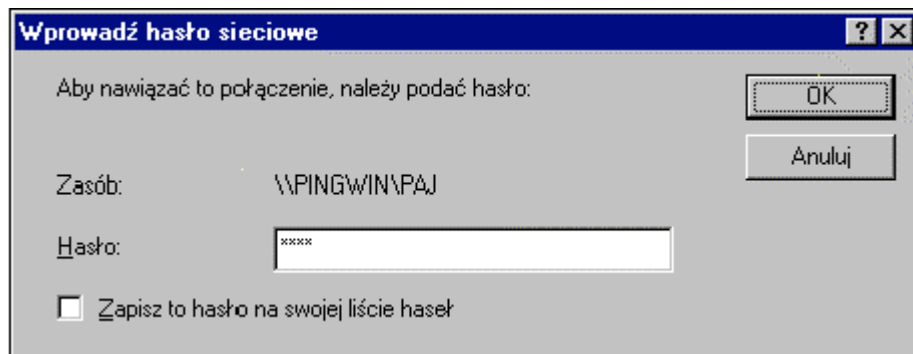
Mapowanie litery H: na dysk sieciowy „poligon” pod Windows 2000

W tym przypadku ścieżka (UNC) do zasobu to \\pingwin\poligon. Po naciśnięciu przycisku „Zakończ” z dysku H: będzie można korzystać jak z każdego innego, lokalnego dysku twardego. Przydatna jest także opcja „Połącz ponownie przy logowaniu” – dzięki niej po każdym uruchomieniu komputera nastąpi automatyczne połączenie z zasobem i przypisanie mu dyskowej literki H:

W przypadku łączenia się z katalogiem domowym na serwerze, ścieżkę UNC można symbolicznie zapisać jako \\zdalny_komputer\nazwa_uzytkownika:



Mapowanie litery H: na katalog domowy pod Windows 98



Autoryzacja użytkownika przy próbie łączenia się z katalogiem domowym

Przy próbie łączenia się z katalogiem domowym użytkownik proszony jest o wpisanie hasła w celu autoryzacji. Aby odłączyć dysk sieciowy wystarczy (np. w Eksploratorze) kliknąć na nim prawym przyciskiem myszki i z menu kontekstowego wybrać „Odłącz”.

Mapowanie dysku jest w systemie Windows możliwe także w trybie tekstowym. Poleceniem, które to umożliwia jest net.exe. Poniższe przykłady wykonują te same czynności, które wyżej zostały wykonane w trybie graficznym.

- mapowanie litery H: na dysk sieciowy „poligon”:
net use h: \\pingwin\poligon
- mapowanie litery H: na katalog domowy użytkownika paj:
net use h: \\pingwin\paj
- odłączenie dysku sieciowego H:
net use h: /d

11. Zasoby dla grupy użytkowników

Stosunkowo często zachodzi potrzeba udostępnienia jakiegoś zasobu dla grupy użytkowników. Przykładem mogą być dane udostępniane jedynie księgowym, grupie znajomych administratora czy grupie ludzi pracujących nad jednym projektem. Samba umożliwia definiowanie grupy użytkowników, którym taki dostęp przysługuje.

Utworzenie przykładowej grupy pod Linuxem jest proste i wykonuje się je za pomocą polecenia groupadd. Aby dodać do grupy nowych użytkowników, należy wykonać polecenie usermod z odpowiednimi opcjami. W celu utworzenia grupy księgowość oraz dodania do niej użytkowników tomek, anna i jacek należy wykonać:

```
groupadd ksiegowosc
usermod -G ksiegowosc tomek
usermod -G ksiegowosc anna
usermod -G ksiegowosc jacek
```

Pozostało jeszcze tak skonfigurować Sambę, aby tylko tym użytkownikom udostępniła określony zasób. Parametrem, który to umożliwia jest `valid users`. Przykładowy wpis w pliku `smb.conf` wygląda tak:

```
[finanse]
comment = Dokumenty księgowych
path = /mnt/sprawy_finansowe
writable = yes
valid users = paj +ksiegowosc
force group = ksiegowosc
```

Powyższa sekcja udostępnia lokalny katalog `/mnt/sprawy_finansowe` grupie `ksiegowosc` oraz użytkownikowi `paj`. W „otoczeniu sieciowym” zasób ten widziany jest jako `finanse`. Zwracam uwagę na fakt, że przed nazwą grupy należy postawić znak „+” (plus). Wartościami tego parametru mogą być nazwy użytkowników i nazwy grup. Katalog udostępniany grupie, powinien mieć lokalnie ustawione prawa zapisu i odczytu dla całej grupy.

Parametr `force group` powoduje, że każdy użytkownik (`tomek`, `anna`, `jacek`, `paj`), który połączy się z zasobem, będzie przez Sambę widziany jako użytkownik grupy `ksiegowosc`. Umożliwi to prawo zapisu do tego folderu i użytkownikom tej grupy i użytkownikom nie będącym członkami tej grupy.

12. Inne przydatne parametry

Samba dysponuje dziesiątkami, jeśli nie setkami, parametrów. Praktyczne zastosowanie znajduje jednak mała część z nich. Przedstawię te, które do tej pory nie zostały wykorzystane, a które mogą znaleźć zastosowanie w większości konfiguracji.

read only

jest parametrem, o którym wcześniej już wspominałem. Umożliwia on ustawienie zasobu w tryb „tylko do odczytu”. Może pełnić ciekawą rolę w połączeniu z kolejnym parametrem.

write list

określa on listę użytkowników, którzy otrzymują prawo do zapisu (i odczytu) nawet wówczas, gdy zasób udostępniony jest „tylko do odczytu”.

Praktycznym zastosowaniem powyższych parametrów w sieci lokalnej może być udostępnienie katalogu, w którym znajdują się istotne informacje, np. dla pracowników lub znajomych. Z oczywistych przyczyn folder udostępniany jest tylko do odczytu, natomiast prawa do jego modyfikacji przysługują jedynie upoważnionej osobie.

Oto przykład konfiguracji:

```
[urlopy]
comment = Terminy przydzielonych urlopow
path = /mnt/urlopy
read only = yes
write list = paj
guest ok = yes
```

Udostępniony folder zawiera informacje o wolnych oraz zajętych już terminach urlopów. Jest oczywiste, że prawo do jego modyfikacji powinna mieć upoważniona osoba (w tym przypadku jest nią użytkownik paj). Inni użytkownicy mogą przeglądać te informacje, nie mogą ich jednak modyfikować.

Na podobnej zasadzie można udostępniać terminy spotkań, wyniki testów, różnego rodzaju dokumenty firmowe oraz inne informacje, do których prawa modyfikacji mogą mieć poszczególne osoby lub ich grupy.

max connections

jest parametrem, który określa maksymalną liczbę klientów, którzy mogą dołączyć się do zasobu. Parametrem tym, który może pojawić się zarówno w sekcji [global] jak i każdej innej, można ograniczyć obciążenie serwera. Domyślnie parametr ten przyjmuje wartość zero, co oznacza dowolną liczbę połączeń z Sambą.

time server

jest to parameter sekcji [global], przyjmujący wartość „no” (domyślnie) lub „yes”. W tym drugim przypadku serwer Samba działa jako serwer czasu dla klientów windowsowych. Może znaleźć zastosowanie w sieciach, w których ważna jest synchronizacja czasu między serwerem a klientami. Aby ją przeprowadzić, należy pod Windows wykonać polecenie net time z opcjonalną nazwą serwera poprzedzoną dwoma lewymi ukośnikami.

preexec, postexec

parametry te definiują polecenia, które wykonywane są na serwerze, po połączeniu z określonym zasobem. Pierwszy z nich wykonywany jest przy połączeniu, drugi natomiast przy rozłączeniu.

Przykładowym zastosowaniem powyższych jest udostępnienie napędu CD-ROM na serwerze. Pod Linuxem, przy każdej zmianie płyty należy ją „zamontować”. Dzięki tym parametrom dzieje się to automatycznie:

```
[cd-rom]
comment = CD-ROM na serwerze
writeable = no
preexec = /bin/mount /mnt/cdrom
postexec = /bin/umount /mnt/cdrom
```

Aby polecenia te uruchamiane były jako użytkownik root należy je wywołać w taki sposób: root postexec lub root preexec.

13. Samba jako serwer WINS

W sieciach lokalnych bardzo często zachodzi potrzeba odwzorowania nazwy komputera na jego adres - wówczas przeważnie wpisywana jest nazwa komputera widoczna w „otoczeniu sieciowym”. W rzeczywistości nic ona komputerowi nie mówi, i zanim połączy się on z żądanym zasobem musi przekształcić podaną nazwę (np. pingwin) na odpowiedni adres.

W sieci bez serwera nazw dzieje się to przy pomocy rozgłoszeń. Oznacza to, że komputer poszukujący innego, wysyła do wszystkich komputerów pracujących w podsieci zapytanie „kto ma taką nazwę?”. Dopóki sieć lokalna jest niewielka, nie powoduje to żadnych problemów (prócz zwiększonego ruchu w sieci). Schody zaczynają się wówczas, gdy sieć zaczyna się rozrastać lub zbudowana jest z urządzeń, które nie przepuszczają adresów rozgłoszeniowych. Oczywiście przy większej sieci zwiększa się także natężenie ruchu.

Aby rozwiązać ten problem, Microsoft opracował usługę Windows Internet Name Service (WINS), czyli serwer nazw dostępny z wielu podsieci. Każdy komputer pojawiający się w sieci rejestruje swoją nazwę na serwerze WINS. Jeśli zachodzi potrzeba odwzorowania nazwy na adres, prośba o to kierowana jest od razu do serwera WINS. Wynikają z tego same korzyści: brak niepotrzebnego ruchu sieciowego, natychmiastowa odpowiedź serwera, brak kłopotów związanych z ograniczeniem zasięgiem adresów rozgłoszeniowych oraz pewność, że w sieci nie pojawią się dwa komputery o tej samej nazwie.

Samba potrafi emulować serwer WINS i skonfigurowanie jej do pełnienia tej funkcji ogranicza się w gruncie rzeczy do jednego parametru w sekcji globalnej:

```
wins support = yes
```

Na uwagę w tym miejscu zasługuje parametr name resolve order. Ustala on kolejność, w jaki serwer Samba spróbuje przetłumaczyć zapytanie. Domyślnym ustawieniem jest:

```
name resolve order = lmhosts host wins bcast
```

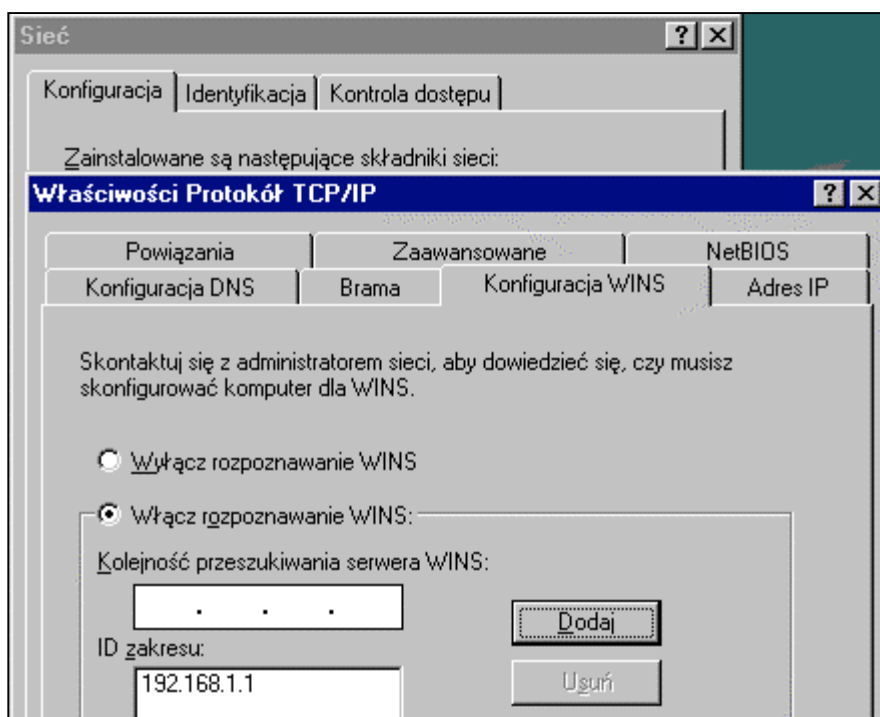
Pierwszy z nich oznacza, żeby najpierw szukać odwzorowania w pliku lmhosts. W przypadku niepowodzenia należy go szukać w pliku hosts (druga wartość). Następnie Samba wykorzysta zgłoszenia ze swojej aktualnej bazy danych WINS. W ostateczności, gdy i to nie przyniesie rezultatu, roześle ona zapytanie do wszystkich komputerów w podsieci tak, jakby serwer WINS nie istniał.

Pliki lmhosts (domyślnie znajduje się w /usr/local/samba/lib/) oraz hosts (domyślnie w /etc/) mają podobną składnię: adres_komputera jego_nazwa. Jedyną różnicą między nimi jest to, że pierwszy z nich przechowuje nazwy NetBIOS - „otoczenia sieciowego” (np. mające ograniczenie długości do 15 znaków) a drugi z nich może zawierać pełne nazwy DNS.

Aby komputery pracujące pod Windows zaczęły korzystać z serwera WINS, należy:

a) w Windows 98

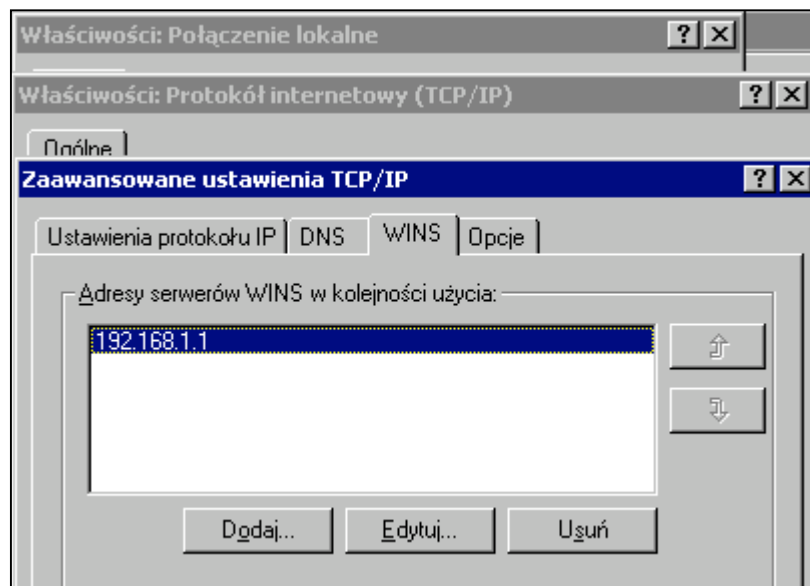
Po kliknięciu prawym przyciskiem myszki na ikonie „Otoczenie sieciowe” należy wybrać Właściwości. Kolejnym krokiem jest wybranie właściwości protokołu TCP/IP. Adres IP serwera WINS wpisuje się po wybraniu zakładki „Konfiguracja WINS”.



Konfiguracja Windows 98 do korzystania z serwera WINS

b) w Windows 2000

Po kliknięciu prawym przyciskiem myszki na ikonie „Moje miejsca sieciowe” należy wybrać Właściwości, następnie kliknąć prawym przyciskiem na „Połączeniach lokalnych” i wybrać Właściwości. Kolejnym krokiem jest wybranie właściwości protokołu TCP/IP. Po kliknięciu na przycisku Zaawansowane należy wybrać zakładkę WINS.



Konfiguracja Windows 2000 do korzystania z serwera WINS

Komputer może także automatycznie pobrać adres serwera WINS, jeśli swoje ustawienia sieciowe pobiera z serwera DHCP.

14. Przeglądanie w sieci lokalnej

Do przeglądania sieci lokalnej (oraz zasobów w niej dostępnych) użytkownicy Windows wykorzystują „Otoczenie sieciowe” (można użyć także polecenia net view z linii poleceń). Po uruchomieniu tego narzędzia dostępna jest lista obecnych w sieci komputerów.

W praktyce przeglądanie obsługiwane jest przez systemy pełniące rolę serwerów przeszukiwania. Serwer taki przesyła do klienta listę wszystkich dostępnych w sieci komputerów. List ta modyfikowana jest przez serwer na bieżąco dzięki komunikatom wysyłanym przez wszystkie komputery będące aktualnie w podsieci.

Jeśli serwer przeglądania przestaje być dostępny w sieci, uruchomiony zostaje proces elekcji – proces, który ma na celu wyłonienie głównej przeglądarki. Elekcja może zostać także zapoczątkowana przez wysłanie odpowiedniego komunikatu przez dowolny system z sieci Windows. Na wynik tego procesu wpływ ma przede wszystkim wartość „poziomu systemu operacyjnego” OS Level, która zostanie omówiona niżej.

Samba może z powodzeniem pełnić rolę przeglądarki głównej w sieci Windowsowej dzięki czemu inne komputery nie muszą przeznaczać ani swojej pamięci ani czasu procesora do obsługi listy przeglądania. Nadto lista ta dostępna jest od razu na serwerze linuxowym.

Aby Samba zaczęła pełnić w sieci rolę głównego serwera przeszukiwania, należy w sekcji [global] pliku smb.conf dopisać kilka parametrów:

```
local master = yes
preferred master = yes
os level = 65
```

local master

parametr ten ustala, czy Samba powinna próbować zostać główną przeglądarką w sieci (czyli brać udział w elekcji).

preferred master

określa, czy w serwer powinien rozpocząć proces elekcji w momencie pojawienia się w sieci oraz w sytuacji, gdy nie jest on główną przeglądarką.

os level

to parametr, który definiuje wartość OS Level (wspomniałem o niej wcześniej). Elekcję wygrywa system, u którego wartość ta jest największa. Warto wspomnieć o tym, że wartość ta w przypadku np. Windows NT Server wynosi 32 a dla Windows 95 równa jest 1. Maksymalna wartość tego parametru wynosi 255, jednak zalecaną (i domyślną) wartością jest 65.

Jako ciekawostkę dodam, że jeśli w procesie elekcji dochodzi do remisu, brane pod uwagę są wartości takich elementów jak długość czasu pobytu komputera w sieci czy jego nazwa (decyduje porządek alfabetyczny).

15. Ograniczenie dostępu do Samby

Na początek posłużę się przykładem, który odczułem na własnej skórze. Dzięki niemu zawsze pamiętam kwestię (stosunkowo prostego) zabezpieczenia serwera plików przed dostępem z niepowołanych adresów.

Pewnego razu, zaraz po świeżej instalacji Linuxa i szybkiej konfiguracji Samby zaistniała potrzeba połączenia się z Internetem. Po krótkiej konfiguracji modemu połączyłem się z Siecią i spokojnie załatwiałem swoje sprawy. Gdy skończyłem, zauważyłem w logach (dziennikach systemu) połączenie z moją Sambą z jakiegoś miejsca w Sieci, skądś ze świata (jak się później okazało – z Polski).

Mój serwer plików udostępniał wówczas (między innymi) katalog „poligon”, dostępny dla wszystkich. Przed połączeniem z Internetem katalog ten był pusty (jak wcześniej wspomniałem było to zaraz po instalacji Linuxa). Gdy spojrzałem na „poligon” po wyjściu z Sieci ujrzałem tam jeden, nowy plik tekstowy o nazwie, która mówiła wszystko: tu_bylem.txt.

W moim przypadku obeszło się „bez ofiar”, jednak łatwo jest wyobrazić sobie czym mogłaby się skończyć taka wizyta, gdyby „poligon” zawierał np. dokumenty firmowe lub inne ważne informacje. Muszę jeszcze wspomnieć że, połączony byłem wtedy z Internetem około 45 minut...

Popełniłem wówczas dwa błędy – pierwszy z nich polegał na tym, że nie miałem firewall’a, który blokowałby dostęp do Samby z Internetu. Drugim błędem był fakt, że nie zdefiniowałem w pliku smb.conf komputerów, które mogą się z moją Sambą łączyć.

Wracając do Samy – zarówno w sekcji globalnej pliku smb.conf, jaki i dla każdego zasobu niezależnie, można zdefiniować adresy komputerów, które mogą mieć dostęp do udostępnianych danych. Naturalnym wydaje się zezwolenie na połączenia z Sambą z całej sieci lokalnej. Przykładowo, jeśli używane są w niej adresy z zakresu 192.168.1.0 - 192.168.1.255 wpis powinien wyglądać tak:

```
hosts allow = 192.168.1.
```

Na podobnej zasadzie, lecz o przeciwnym znaczeniu, działa parametr hosts deny. Można także wykluczyć poszczególne komputery posługując się słowem kluczowym EXCEPT. Poniższy zapis w pliku smb.conf nie pozwoli na połączenia komputerom o adresach IP 192.168.2.0 - 192.168.2.255 za wyjątkiem hosta 192.168.2.5:

```
hosts deny = 192.168.2. EXCEPT 192.168.2.5
```

W przypadku konfliktu powyższych parametrów pierwszeństwo ma hosts allow. Aby uniemożliwić dostęp do zasobu konkretnemu użytkownikowi (ew. grupie użytkowników) należy posłużyć się parametrem invalid users. Poniższy przykład ilustruje odebranie użytkownikowi heniek tych praw:

```
invalid users = heniek
```


16. Pliki dziennika

Najwięcej informacji dotyczących pracy Samby znajduje się w dzienniku tego programu, tworzonym na bieżąco. Informacje te znajdują szczególne zastosowanie przy diagnozowaniu serwera oraz usuwaniu problemów.

Oto przykładowy wpis, który należy umieścić w sekcji [global] pliku smb.conf:

```
log file = /var/log/samba/samba.%m
log level = 1
max log size = 40
```

log file

Parametr ten określa katalog oraz nazwę pliku w którym zapisywane będą „logi”. Zmienna %m oznacza, że dla każdego komputera w sieci lokalnej, utworzony zostanie osobny plik dziennika. Na przykład próby łączenia się z Sambą z komputera arek zostaną zapisane w pliku samba.arek. Podanie jednoznacznej nazwy pliku (bez zmiennych) spowoduje zapisywanie wszystkich informacji w tymże pliku.

log level

Określa poziom rejestrowania informacji diagnostycznych. Może on zmieniać się od 1 do 10, przy czym poziom 1 zapewnia niewiele informacji, a poziom 10 - bardzo dużo. Jeśli Samba działa prawidłowo, wystarczającym poziomem jest 1. Wyższe wartości należy stosować w przypadku problemów. Nie zaleca się jednak przekraczanie poziomu trzeciego.

max log size

Określa maksymalny rozmiar pliku w kilobajtach. Jeśli rozmiar ten przekroczy podane maksimum, Samba zmieni jego nazwę dodając rozszerzenie .old.

17. Drukarka plików .pdf

Pliki z rozszerzeniem .pdf (*ang. Portable Document Format*) mają wiele niezaprzeczalnych zalet:

- można je bez problemów odczytać pod różnymi systemami operacyjnymi
- posiadają stosunkowo niewielką objętość
- dokumentacja sprzętu jak i oprogramowania bardzo często występuje w tym formacie
- przeglądarki (*viewery*) plików .pdf są darmowe (nawet pod Windows !)

Tak więc firmie Adobe (bo chyba ona opracowała ten format) udało się stworzyć niezłe cacko. Jedynym problemem są programy tworzące te pliki, gdyż są to programy komercyjne. Prawie wszystkie :)

Aby tworzyć „legalne” PDFy wystarczy Linux, Samba i pakiet GhostScript. Ten ostatni jest dostarczany chyba z każdą dystrybucją Linuxa, dlatego albo go doinstaluj albo pobierz sobie i zainstaluj najnowszą wersję (<http://www.ghostscript.com>). Główną rolę będzie pełnił plik ps2pdf, będący częścią tego pakietu.

W tym miejscu chciałbym podziękować Bartłomiejowi S., który podesłał mi praktycznie gotowe rozwiązanie tego zagadnienia (pozdrawiam Kielce).

- a) tworzymy plik `/usr/local/bin/printpdf` i dajemy wszystkim prawa do jego wykonywania:

```
cd /usr/local/bin
touch printpdf
chmod a+x printpdf
```

- b) tworzymy katalog `/mnt/pdf`, jego właścicielami niech będą `nobody` i `nogroup`. Niech tylko oni mają do niego prawa (pełne):

```
mkdir /mnt/pdf
chmod 0700 /mnt/pdf
chown nobody:nogroup /mnt/pdf
```

- c) W pliku `/usr/local/bin/printpdf` umieszczamy, co następuje:

```
#!/bin/sh
#
# by John Bright, 2001, jbright@winfordeng.com
DATE=`date +%b%d-%H%M%S`
TARGETDIR=/mnt/pdf
ps2pdf $1 $TARGETDIR/$DATE.tmp
mv $TARGETDIR/$DATE.tmp $TARGETDIR/$DATE.pdf
rm $1
```

- d) W pliku konfiguracyjnym `smb.conf` umieszczamy drukarkę oraz odpowiedni katalog:

```
# drukarka sieciowa plików .pdf
[make_pdf]
path = /tmp
printable = yes
guest ok = yes
print command = /usr/local/bin/printpdf %s

# katalog, w którym udostępnione będą wygenerowane .pdfy
[pdfy]
path = /mnt/pdf
guest ok = yes
browsable = yes
writable = yes
```

- e) Dodajemy do Windows drukarkę sieciową z wbudowaną obsługą PostScriptu (np. HP LaserJet 5P/5PM PostScript). Ścieżka do niej to oczywiście `\\pingwin\make_pdf`. Po wydrukowaniu do niej czegokolwiek, np. strony testowej drukarki, w „otoczeniu sieciowym”, na pingwinie, w zasobie „pdfy” powinniśmy odnaleźć plik z rozszerzeniem `.pdf`.

Uwagi:

- `nobody` i `nogroup` to użytkownicy „goście”. Jeśli Samba wpuszcza kogoś bez konieczności podania hasła zakłada, że ma do czynienia z `nobody` (bez obrazu :).
- w skrypcie `printpdf` apostrofy przy zmiennej `DATE` znajdują się przeważnie po lewej stronie klawisza z cyfrą 1.
- możesz sobie zmienić katalog docelowy oraz odpowiednie prawa, nazwę powstałych plików `.pdf` na jakie tylko chcesz. Tylko zrób to poprawnie.

18. Samba – kontroler domeny dla Windows 9x

Nie wnikając w szczegóły: Samba skonfigurowana jako podstawowy kontroler domeny (*ang. PDC: Primary Domain Controller*) świetnie sprawdza się w biurze, firmie itp. Oto najbardziej praktyczne plusy:

- w momencie logowanie się użytkownika do Windows, jego hasło sprawdzane jest na serwerze Samby. Nikt nie uzyska dostępu do jej zasobów, jeśli nie ma konta w pliku z hasłami (np. `/etc/smbpass`). W ten sposób można wydzielić swoiste zamknięte „otoczenie sieciowe” w ogólnodostępnym „otoczeniu sieciowym”
- użytkownik podaje swój login i hasło tylko raz (w momencie logowania się do Windows). Od tego momentu Samba wpuści go do wszystkich zasobów (do których ma prawo) bez konieczności podawania za każdym razem hasła. W naszym przykładzie użytkownik paj nie będzie pytany o hasło ani w momencie dostępu do swojego katalogu domowego, ani w momencie dostępu do zasobu udostępnionego dla grupy, do której należy itd.
- w momencie logowania się użytkownika do domeny, można uruchomić skrypt, który uruchomiony zostanie na jego komputerze. Można więc zrobić tak, żeby po każdym jego zalogowaniu się (bez względu na to, z którego komputera) dysk H: mapowany był na katalog domowy użytkownika, dysk Z: na „poligon” itp. Można też automatycznie formatować mu np. dysk twardy – wszystko zależy od potrzeb i możliwości plików wsadowych `.bat` działających pod Windows oraz wyobraźni admina
- uwaga teraz: za użytkownikiem może po sieci (tj. domenie) wędrować ustawienie jego pulpitu, menu start, skrótów itp. – są to tzw. profile. Tak więc bez względu na fakt, na którym komputerze zaloguje się pani Zosia, na swoim pulpicie zawsze będzie miała te same ikony, te same menu i tak do znudzenia ;)

Dobra, wystarczy tych plusów. Opiszę tutaj powyższe dla komputerów pracujących pod Win 9x. Dla NT/2000 jest to trochę bardziej skomplikowane i nie wiem, czy ktokolwiek to w ogóle czyta...

Zaczynamy: za chwilę zmienimy grupę roboczą na domenę. Jedną z różnic między nimi polega na tym, że PDC pracuje w trybie bezpieczeństwa użytkownika a nie zasobów. W praktyce oznacza to tyle, że trzeba dodać parę wpisów w `smb.conf`. A tak poważnie: bez konta na Sambie, użytkownik nie zostanie do niej wpuszczony. Do dzieła!

18a Samba jako PDC

Najpierw skonfigurujemy Sambę jako PDC. Chodzi tylko o to, żeby można było się zalogować do odpowiedniej domeny z poziomu Windows 9x a następnie nie być pytanym o hasło przy dostępie do zasobów, do których mamy prawa. Oto przykładowy smb.conf:

```
[global]
    # tryb bezpieczeństwa użytkownika - niezbędne
security = user
    # teraz „workgroup” to nazwa domeny
workgroup = domena
    # kontroler domeny – niezbędne
domain master = yes
domain logons = yes
encrypt passwords = yes
smb passwd file = /etc/smbpass

    # inne potrzebne
local master = yes
preferred master = yes
os level = 90

    # pierdoły
netbios name = pingwin
log file = /var/log/samba.log
log level = 2
character set = ISO8859-2
client code page = 852

    # zasób, który musi istnieć, nie musi nic zawierać: netlogon
[netlogon]
path = /mnt/netlogon
writeable = no
public = no

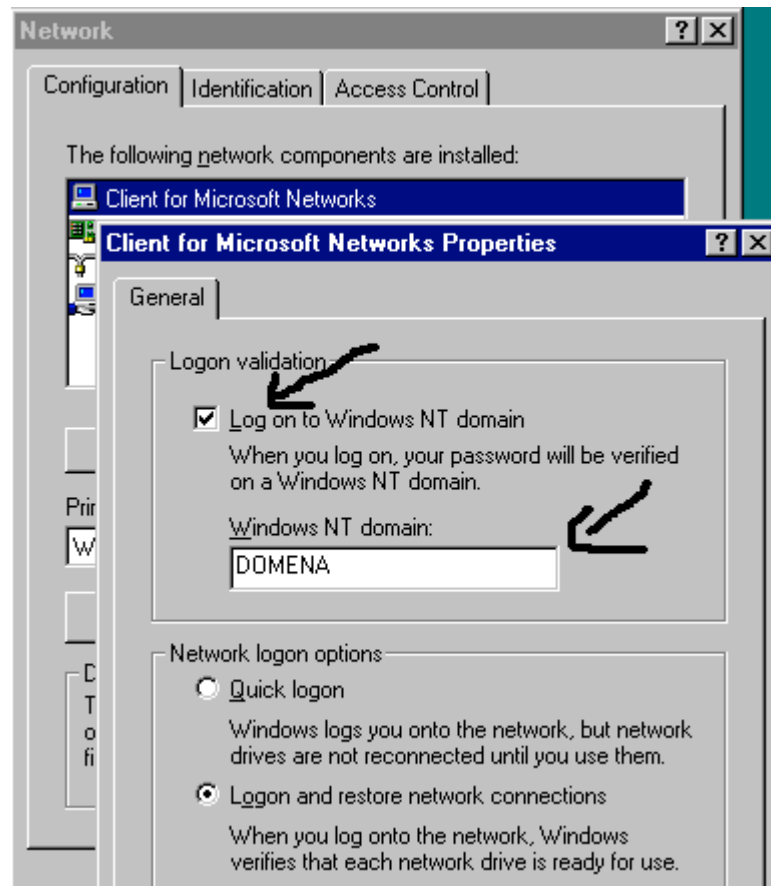
    # coś trzeba udostępnić...
[homes]
writeable = yes
```

Teraz parę słów wyjaśnień: dla Samby jako PDC hasła muszą być szyfrowane i przechowywane w oddzielnym pliku. To, o co tu chodzi wyjaśniam w punkcie 8. Zanim nie będziesz pewien, że toto wszystko działa jak należy, ustaw sobie logowanie jak wyżej i patrzaj co chwilę logi. Przed odpaleniem Samby, wykonaj testparm. No i jeszcze netlogon: stwórz sobie jakkolwiek katalog, i udostępnij go pod nazwą [netlogon]. Do czegoś takiego odwołują się Windy przy logowaniu do domeny.

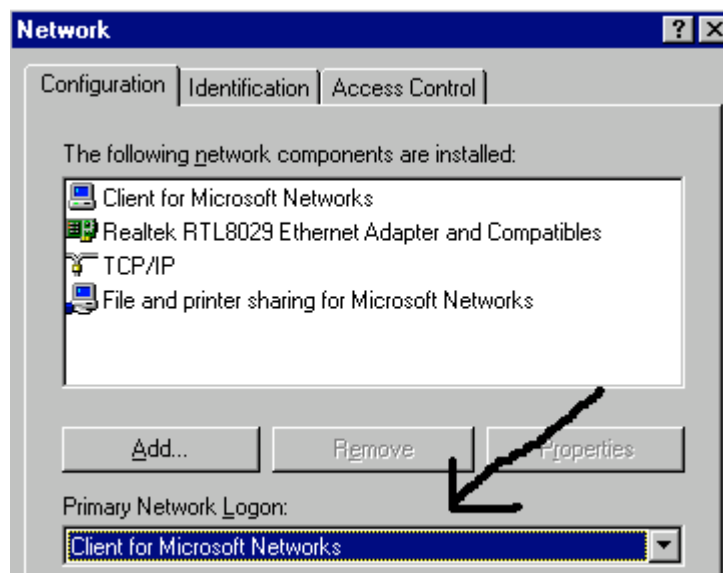
No i jeszcze jedno: utwórz plik z hasłami i dodaj do niego kilku userów (8 punkt). Dobrze by było, gdybyś udostępnił chociażby katalogi domowe userom...

Teraz wykonaj testparm, popraw błędy, przeładuj Sambę, spójrz w logi i siadaj do Win\$hita 9x. Tu powinno pójść szybko i (przy odrobinie szczęścia) bez blue screenów...

Wejdź na „właściwości sieci” i kliknij dwa razy na „Client for Microsoft Networks” („Klient Microsoft Networks” o ile dobrze pamiętam – ostatnio zmieniłem 98 PL na 98 EN. Jedno i drugie to gówno). Powinieneś zrobić coś takiego:



Przygotowanie Windows 9x do logowania się do domeny



Nie zapomnij o tym !!!

Jeśli chcesz uniknąć dziwnych zachowań Windows (o ile to w ogóle jest możliwe), wybierz także „Klient Microsoft Networks”.

Strzałki pokazują, co zmienić. Oczywiście nazwa domeny odpowiada parametrowi workgroup w smb.conf. Potem ok i tradycyjny już reset. Po przeładowaniu, powinieneś zdziwić się - bo wszystko poszło jak należy lub wręcz przeciwnie. W drugim przypadku popatrz w logi i popraw błędy. Sprawdź składnię smb.conf z tym co napisałem wyżej, wykonaj testparm, sprawdź czy istnieje netlogon, plik z logami itd.

Zobacz, czy przez „otoczenie sieciowe” możesz wejść na PDC i swój katalog domowy (bez podania hasła).

Tak czy siak, w końcu Ci się uda. Idziemy dalej...

18b Skrypcik i porządki

Co za debilna nazwa podpunktu...

Skrypcik to tutaj plik wsadowy – czyli taki o rozszerzeniu .bat. Jest on znany wszystkim użytkownikom M\$ DOS. Możemy zrobić tak, aby po każdym udanym przyłączeniu się użytkownika do domeny, na jego komputerze wykonany był automatycznie jakiś .bat. Może on być taki sam dla wszystkich lub indywidualny – w zależności od użytkownika. Ale po kolei...

Najpierw utwórz jakikolwiek plik wsadowy: tutaj utworzę plik mapuj.bat, który każdemu komputerowi zamapuje na dysk H: katalog domowy odpowiedniego użytkownika. Oto, co zawiera wspomniany plik:

```
echo „Witaj w naszej firmie. Dlaczego znowu się spóźniłeś do pracy ?”
net use h: \\pingwin\homes
pause
```

Teraz kilka ważnych uwag: po pierwsze pause występuje tylko po to, żebyś mógł zobaczyć ewentualny komunikat o błędzie. Jeśli wszystko zadziała, pause możesz z niego wyrzucić. U mnie na przykład dysk Z: „był zajęty”, choć Windows „nie widzi” żadnego napędu Z: - nie można na niego wejść, nie istnieje po prostu. Ale Windowsowi coś odjechało i stwierdził że mi nie da literki Z:. Tak więc nie wszystko jest oczywiste.

Po drugie: plik wsadowy, pobrany i uruchomiony z serwera, musi zawierać znaki nowego wiersza z DOS/Windows. Chodzi o to, że systemy te inaczej kodują parę rzeczy, niż Unixy. Najlepiej będzie, jak na początek utworzysz danego .bat pod Windowsem, sprawdzisz, czy działa i przerzucisz go na serwer.

Po trzecie: mapowanie dysków opisuję w punkcie 10.

Jak właśnie wspomniałem, plik mapuj.bat (nazwij go jak chcesz) należy wrzucić na serwer. Dokładnie: do zasobu [netlogon]. W tym przypadku będzie to /mnt/netlogon/.

Pozostało poinformować Sambę, żeby przekazywała ten plik do wykonania przez każdego podłączającego się do domeny klienta. Wystarczy do sekcji global dopisać:

```
logon script = mapuj.bat
```

W sumie to tyle. Można w tym .bat umieścić mapowanie na Z: dysku „poligon” lub dokumentów firmowych, jeśli użytkownik ma do niego prawa odczytu.

Tak więc mapuj.bat wykonany będzie na komputerach wszystkich użytkowników. A co, jeśli Heniek chce automatyczne mapowanie domowego, Ania chce katalog domowy na G: a Czesiu chce „poligon” zamapowany trzy razy, jako F G i H ? Wówczas należy im to wybić z głowy.

Można też utworzyć indywidualne pliki .bat wykonywane przy podłączeniu. Wtedy zamiast zmieniamy wartość logon script na:

```
logon script = %U.bat
```

Spowoduje to zastąpienie %U przez nazwę użytkownika i wywołanie odpowiedniego pliku wsadowego z zasobu [netlogon]. Czyli dla Ani, Heńka i Czesia będą to ania.bat, heniek.bat i czesiek.bat.

Dobra, czaisz o co chodzi więc nie będę się dalej produkował na ten temat. Kawa mi już wystygła...

Teraz trochę o sprzątnięciu, wspomnianym w tytule podpunktu. Chodzi mi o to, że jeśli wejdiesz w „otoczenie sieciowe” na PDC, zobaczysz „homes” i „netlogon”. Pierwszy masz i tak zamapowany a do drugiego i tak nie masz dostępu (przynajmniej nie powinienes). Tak czy siak, jest syf. A syf na serwerze jest gorszy, niż syf w mieszkaniu (możesz mnie cytować). Wracając do tematu: wystarczy w sekcji [homes] i [netlogon] dopisać:

```
browseable = no
```

Tyle na ten temat. Aha, czasami po przeładowaniu Samby Windows nie będzie chciał się zalogować. Oczywiście trzeba go wtedy zresetować :)

Idę zajarać...

18c Podążaj za mną, pulpicie!

Wróciłem. Pani Zosi bardzo by się podobało, gdyby oprócz katalogu domowego mapowanego zawsze na H: także pulpit i inne badziewia były takie same bez względu na to, na którym kompie się zaloguje.

Właśnie sobie coś przypomniałem, chwilowa zmiana tematu: każąc użytkownikom pracować na ich koncie domowym na PDC, zamiast na „Moich dokumentach” możemy zwiększyć bezpieczeństwo danych userów, poprzez robienie kopii zapasowych na serwerze. Wówczas, gdy pani Czesia przyleci spanikowana: „przez pomyłkę nadpisałam plik dwa_tygodnie_mojej_pracy.doc” możemy powiedzieć jej „jeśli postawisz skrzynkę piwa, może uda się coś odzyskać”. Wtedy sięgamy do wczorajszych .tar.gz i wyciągamy z nich te dwa tygodnie pracy pani Czesi.

Wracamy do wędrujących po sieci lokalnej indywidualnych ustawieniach użytkowników. Są to „profile”. Sambę można skonfigurować tak, aby obsługiwała je jak należy.

Wystarczy w sekcji [global] dopisać:

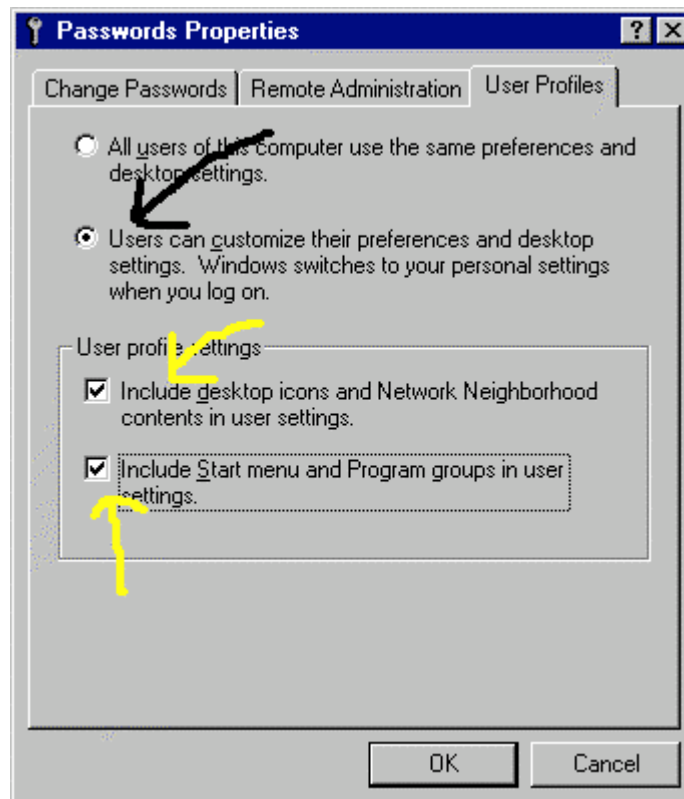
```
logon home = \\%N%\profil_windows
```

Ta właśnie opcja mówi klientowi Windows, gdzie trzymać profil. Tutaj zostanie on utworzony przez Sambę w katalogu domowym użytkownika, w podkatalogu profil_windows.

Ważna uwaga: Pisząc punkt 18 (ten, który właśnie czytasz) wykorzystuję Sambę wersji 2.2.6. We wcześniejszych wersjach (nie wiem dokładnie do której) rolę tę pełnił parametr logon path. Obecnie jest on wykorzystywany przez NT, natomiast Windows 9x wykorzystuje logon home.

Testujemy teraz Sambę (testparm, przeładowanie demonów, plik z logami) i sprawdzamy, czy wszystko o.k. Jeśli tak – bierzemy się za Winę.

Domyślnie Windows ustawiony jest tak, że wszyscy użytkownicy używają tych samych ustawień menu, pulpitu itp. Przydałoby się zmienić to zachowanie i Windows je umożliwia (za darmo!). W Panelu Sterowania należy wybrać Passwords (Hasła) a następnie kliknąć na zakładkę User Profiles (Profile użytkownika).



Indywidualne profile niedługo zaczną działać...

Czarna strzałka wskazuje to, co należy zaznaczyć a żółte ustawienia opcje, które mogą być personalizowane. Chyba trochę przesadzam...

Po szybkim resecie wszystko powinno działać. Od tej pory sprawa wygląda tak: użytkownik loguje się na PDC i pobiera z niego swój profil. Przy wylogowaniu czynione są odpowiednie zmiany na PDC (aktualizacja profilu). Teraz wystarczy iść, zalogować się na innym komputerze i możemy pracować na nim jak na swoim. Faaajne, co ?

A teraz trochę rozważań nad wędrującymi profilami. Niektórzy proponują trzymanie profili w osobnym, niezależnym katalogu. Oto przykład takiej konfiguracji:

```
logon home = \\%N\profile_windows\%U
```

```
[profile_windows]
comment = Profile Windows
path = /mnt/profile
create mode = 0600
directory mode = 0700
writeable = yes
# browseable = no
```

Można zrobić i tak, ale:

- albo katalog /mnt/profile musi mieć prawa zapisu dla wszystkich (jeśli użytkownicy nie pracują na serwerze np. poprzez ssh, jest to chyba najlepsze rozwiązanie)
- albo trzeba dla każdego użytkownika ręcznie utworzyć w nim podkatalog nadając prawa 0700 i zmieniając właściciela (dobre rozwiązanie, gdy nie masz wielu użytkowników)

I jedno i drugie rozwiązanie ma swoje plusy i minusy. Wszystko zależy od tego, jakim serwerkiem zarządzasz.

19. Rozwiązywanie problemów

Uważam, że problemy związane z Sambą najszybciej rozwiązuje się korzystając z dziennika programu oraz jego dokumentacji. Poniżej przedstawiam kilka narzędzi, mogących pomóc w rozwiązaniu ewentualnych problemów.

Bardzo ważnym programem dostarczanym wraz z Sambą jest testparm. W większości przypadków nie wymaga on podania żadnych argumentów. Wynikiem jego działania jest sprawdzenie poprawności pliku konfiguracyjnego smb.conf oraz wypisanie parametrów Samby wraz z ich wartościami.

Aby upewnić się, że demon smbd działa poprawnie, należy połączyć się z Sambą z komputera, na którym jest ona zainstalowana. Służy temu polecenie smbclient, natomiast wywołanie wygląda następująco:

```
smbclient -L localhost -N
```

W rezultacie program zwróci listę zasobów udostępnianych przez Sambę (przedstawia to poniższy rysunek). Aby upewnić się, że demon nmbd pracuje poprawnie, należy wydać następujące polecenie:

```
nmblookup _ pingwin _
```

W tym przypadku Samba pracuje na komputerze „pingwin”. Wynikiem tak zadanego polecenia powinien być zwrócony adres IP komputera, podanego jako parametr.

Uważam, że dokumentacja dostarczana razem z kodem źródłowym jest wystarczająca do rozwiązania większości problemów. Zauważyłem także, że pytania dotyczące programu, pojawiające się na grupie dyskusyjnej pl.comp.os.linux nie pozostają bez odpowiedzi.

20. Podsumowanie i posłowie

Opisałem tutaj konfigurację Samby, która umożliwia:

- zaistnienie Linuxa w „otoczeniu sieciowym”
- udostępnienie katalogu z prawami odczytu/zapisu dla wszystkich
- udostępnienie katalogów domowych użytkownikom
- udostępnienie zasobu grupie użytkowników
- działanie Samby jako serwera WINS
- działanie Samby jako przeglądarki w sieci lokalnej
- „drukowanie” do pliku .pdf
- skonfigurowanie Samby jako PDC

Opisałem pokrótce sprawy związane z instalacją programu, jego diagnozowaniem oraz poruszyłem kwestię bezpieczeństwa w kontekście dostępu do danych udostępnianych przez serwer.

Jest to pierwsza wersja tego dokumentu i zawiera pewnie jakieś błędy / niedoróbki / potknięcia itp. Będę bardzo wdzięczny za wszelkie uwagi, komentarze, poprawki, wyrazy wdzięczności. Z góry przepraszam za powyższe i mam nadzieję, że będziecie mnie informować w których miejscach coś nie gra. Jako (częściowe) wytłumaczenie przedstawiam fakt, że większość tej pracy powstawała w późnych godzinach nocnych.

Kontakt ze mną: linio@terramail.pl

Henryk Liniowski
<http://linio.terramail.pl>
Poznań, 2002
