Freesco Info 2.0

Dokument wg którego ustawiony jest router dostępowy oparty o system Linux FREESCO do internetu oraz serwer SAMBA w Szkole Podstawowej Nr2 w Pile

opiekun pracowni i nauczyciel
Janusz Turczynowicz

I. FREESCO INFO 2.0 - INFORMACJE OGÓLNE.

1.1 Dlaczego powstał ten dokument?
Dokument ten powstał, gdyż użytkownicy grupy *trzepak.freesco*, korzystający z niej od dawna
(nazwijmy ich 'starą gwardią') postanowili skończyć z pojawiającymi się dosyć często pytaniami
dotyczącymi Freesco, które na grupie już dosyć dawno znalazły swoje rozwiązanie, oraz by
w jednym miejscu zgromadzić polskojęzyczną dokumentację dotyczącą wszelkich rozwiązań
oferowanych przez Freesco 0.2.7
1.2 Kto tworzy ten dokument i jak można pomóc?
Jeżeli rozwiązałeś jakiś problem związany z Freesco i wydaje ci się, że warto byłoby jego
rozwiązanie opublikować w FAQ, podeślij problem i opis rozwiązania na adres: lukasz@arx.pl,
lub na adres któregoś z wymienionych powyżej autorów tego dokumentu. Również jeżeli
masz jakiekolwiek inne uwagi bądź też propozycje odnośnie tego dokumentu prosz o kontakt
z którymś z jego autorów.
W chwili obecnej nad dokumentem pracują:
morpheus (lukasz@arx.pl),
cinas (cinas@cinas.mine.nu),
Maciek (maciek@pon.bytow.pl),
Olek (olotest@poczta.onet.pl),
Mis' (mis@hustons.homechoice.co.uk),
oraz inni grupowicze trzepak.freesco
1.3 Gdzie można znaleść najnowszą wersję?
Dokument w najnowszej wersji jest zawsze dostępny na stronach internetowych Polskiej Strony
Freesco (*http://www.freesco.arx.pl*). Informacja o pojawieniu się jego nowej wersji będzie
rozsyłana na grupę dyskusyjną *trzepak.freesco* na serwerze *news://news.trzepak.pik-net.pl/*
oraz być może na inne grupy zbliżone tematycznie do *trzepak.freesco*, oraz grupy takie jak
pl.answers na serwerze *news://news.tpi.pl/*
Najnowszą wersję tego dokumentu znaleść można zawsze pod adresem:
http://www.freesco.arx.pl/faq/freesco_info.pdf - format Adobe Acrobat
http://www.freesco.arx.pl/faq/freesco_info.txt - format TXT (Windows)
http://www.freesco.arx.pl/faq/html/index.htm - w formacie HTML

II. GRUPA DYSKUSYJNA: trzepak.freesco

2.1 Czego dotyczy grupa?
Dyskusja na grupie sprowadza się do rozwiązywania problemów, jakie może napotkać użytkownik dystrybucji Freesco. Grupowicze pomagają sobie w instalacji oraz konfiguracji
Freesco w lokalniej sieci komputerowej, wymieniają poglądy na tematy związane z administracją
serwerami opartymi o dystrybucję Freesco, testują nowe pakiety oprogramowania.
2.2 Netykieta grupy dyskusyjnej trzepak.freesco
Zanim zadasz swoje pytanie na grupie trzy razy sprawdź, czy odpowiedzi na nie nie znajdziesz
w tym dokumencie, w archiwum grupy (*http://www.freesco.arx.pl/news/*), na polskim forum freesco (*http://www.freesco.arx.pl/forum/*), oraz w postach z ostaniego tygodnia na grupie.
Zapoznaj się też z dokumentem *'Mini Netykieta grup news i list dyskusyjnych'* znajdującym się pod adresem: *http://www.pg.gda.pl/~agatek/netq.html*
2.3 Najważniejsze zasady dotyczące zachowania na grupie
Staraj się dobrze sprecyzować swój problem. Pytania w rodzaju: "Freesco nie działa, co mam
teraz zrobić?" mogą bardzo silnie zdenerwować pozostałych uczestników dyskusji, podobnie
jak powtarzajce się kilkukrotnie w ciągu tygodnia te same pytania (zanim więc wciśniesz
przycisk 'Wyślij' postaraj się jeszcze raz poszukać odpowiedzi samemu na stronach, których
adresy zostały podane powyżej),
Pod żadnym pozorem nie wysyłaj na grupę reklam, ogłoszeń, oraz maili w stylu: "potrzebuję
rozwiązania problemu, nie czytam tej grupy więc proszę o odpowiedzi na priv",
W żadnym wypadku NIE wysyłaj swoich postów na grupę w html'u, nie wszyscy używają
Outlooka, pamiętaj też, aby ustawiona praz ciebie w programie do obsługi grup dyskusyjnych
długość linii nie przekraczała 71 znaków, natomiast twój podpis (sygnaturka) nie może mieć
więcej niż 4 linijki,
Jedynym dopuszczalnym standardem kodowania polskich znaczków na naszej grupie jest ISO
8859-2, jeżeli nie możesz się dostosować nie używaj polskich znaków w swoich postach,
Odpisując na list, nie cytuj go w całości, lecz pozostaw tylko to co jest absolutnie niezbędne,
a do czego odnosi się twój komentarz. Szczególnie naganne jest cytowanie czyjegoś podpisu
(sygnaturki). Równie godne potępienia jest zacytowanie listu po to tylko aby dodac pod nim
tekst w stylu: "też tak myslę". Na początku cytatu należy umieścić informacje o jego autorze.
Sam cytat powinien zawsze poprzedzać twój komentarz.

2.4 Gdzie jest archiwum grupy?
Główne archiwum grupy znajduje się pod adresem: *http://www.freesco.arx.pl/news/*
Do części archiwalnych postów można dostać się również z serwisu: *http://njusy.onet.pl*

III. FREESCO - INFORMACJE OGÓLNE

3.1 Dystrybucja Freesco - licencja, autorzy, etc.

Freesco jest dydtrybucją linuxa stworzoną jako darmowa alternatywa dla drogich sprzętowych routerów Cisco (nazwa: freesco = free+cisco). Rozprowadzane jest na zasadach licencji GPL.

W podstawowej wersji dystrybucja Freesco mieści się na jednej dyskietce, i umożliwia uruchomienie routera w małej sieci komputerowej. Jednak autorzy (*http://www.freesco.org*) zadbali o możliwość przeniesienia Freesco na dysk twardy i instalacji pakietów z dodatkowym oprogramowaniem.

3.2 Freesco - gdzie szukać pomocy?

Freesco pomimo tego, iż jest mało znaną w Polsce dystrybucją linuxa, ma dość dużą bazę dokumentacji w języku polskim. Warto zaznaczyć, że w wielu przypadkach w przeciwieństwie do bardzo skomplikowanych manuali innych dystrybucji pisane są bardzo przystępnym i zrozumiałym językiem. Oficjalna Polska Strona Freesco (*http://www.freesco.arx.pl*) posiada wiele pomocnych w prawidłowym uruchomieniu i skonfigurowaniu Freesco materiałów, znaleść tam można również polskie forum (*http://www.freesco.arx.pl/forum/*) na którym można znaleść ciekawe dyskusje. Rozwiązania wielu problemów doszukać można się też w archiwum naszej grupy dyskusyjnej, które znajduje się pod adresem: *http://www.freesco.arx.pl/news/*

W razie kłopotów po pomoc można zwrócić się również na grupie trzepak.freesco na serwerze:
news://news.trzepak.pik-net.pl/

3.3 Polskie strony na temat Freesco.

http://www.freesco.arx.pl - Oficjalna Polska Strona Freesco,
http://www.freesco.arx.pl/news/ - archiwum grupy dyskusyjnej trzepak.freesco,
http://www.freesco.arx.pl/forum/ - polskie forum na temat Freesco,
http://miniwebportal.and.pl - strona domowa Maćka,
http://www.freesco.broadcasting.pl - strona domowa Bartka,
http://www.cinas.mine.nu - strona domowa cinasa,
http://www.linux.freesco.prv.pl - strona o konfiguracji Freesco,

3.4 Polskie zasoby na temat linuxa (ogólnie).

http://www.jtz.org.pl - zbiór HOWTOs (poradników "Jak To Zrobić") po polsku.
http://www.linuxindex.pl - zestawienie linuxowych linków,
http://linux.gnu.pl/ - artykuły poświęcone konfiguracji i administracji systemu.

3.5 Zagraniczne strony na temat Freesco.

Z angielskojęzycznych zasobów przede wszystkim należy wymienić oficjalną stronę Freesco (www.freesco.org). Obecnie ta strona jest w zasadzie martwa, niemniej choćby ze względów sentymentalnych nie można jej tu pominąć. Zawartość archiwum tamtejszego forum została zrekonstruowana i można ja przeglądać pod adresem:
http://pub1.ezboard.com/bfreesco

Obecnie za oficjalną stronę Freesco możemy uznać www.freescosoft.com Jest to miejsce gdzie można znaleźć niemalże każdy program dla Freesco. Również tamtejsze forum jest źródłem rozwiązań niemalże każdego problemu związanego z Freesco. Można tam znaleźć adresy stron wszystkich autorów pakietów dla Freesco jak również linki do innych dostępnych w sieci stron związanych z Freesco.

3.6 Mirrory www.freescosoft.com.

http://www.freescosoft.com/home/home.html - USA Zachodnia Virginia,
http://us-ct.freescosoft.net/home.html - USA Connecticut,
http://us-tx.freescosoft.net/home.html - USA Texas,
http://dk.freescosoft.net/home.html - Dania,
http://se.freescosoft.net/home.html - Szwecja,
http://es.freescosoft.net/home.html - Holandia,
http://www.freescosoft.org/home.html - Niemcy,
http://freescosoft.abidjanville.com/home.html - Francja,
http://thetigger.dyndns.org/freescosoft/home.html - Szwecja,
http://tecknojunky.dyndns.org/freescosoft/home.html - Kanada,
http://freescosoft.avaarsani.ca/home.html - Kanada,

3.7 Światowe zasoby na temat linuxa (ogólnie).

http://www.linux.org - główna strona linuxowa,
http://freshmeat.net - "świeże mięsko" serwis z oprogramowaniem,
http://sourceforge.net - strona ze źródłami programów dla linuxa,
http://www.linuxdoc.org/ - zbiór linuxowej dokumentacji,
i jeszcze dziesiątki tysięcy innych...

Siłą rzeczy możemy tu przedstawić zaledwie kilka linków, wiele więcej uzyskać używając dowolnej wyszukiwarki internetowej (do wyszukiwania w archiwach grup dyskusyjnych polecamy Google - http://www.google.com).

IV. PODSTAWOWA INSTALACJA I KONFIGURACJA FREESCO

4.1 Skąd pobrać potrzebne pliki?

Aby stworzyć dyskietkową wersję dystrybucji Freesco potrzebujemy pobrać dwa pliki. Pierwszy to obraz dyskietki (w zależności od wersji należy pobrać plik: *f4sdi.img* dla łącza SDI, oraz *freesco-027.zip* dla modemowców), oraz drugi plik: *rawrite.zip* służący do nagrania obrazu na dyskietkę.

Adresy plików do pobrania:
http://www.freesco.arx.pl/strona/download/freesco/freesco-sdi.img - plik: freesco-sdi.img
http://www.freesco.arx.pl/strona/download/freesco/freesco-027.zip - plik: freesco-027.zip
http://www.freesco.arx.pl/strona/download/freesco/rawrite.zip - plik: rawrite.zip

4.2 Przenoszenie obrazu dystrybucji na dyskietkę.

Po rozpakowaniu archiwum rawrite.zip uruchamiamy kopiujemy program *rawrite.exe*, oraz obraz Freesco - *f4sdi.img* do przygotowanego wcześniej katalogu. W systemie MS-DOS, bądź też w oknie 'Trybu MS-DOS' w systemie Windows uruchamiamy program: *rawrite.exe*
Po ukazaniu się: *'Enter disk image source file name:'* wpisujemy nazwę pliku z Freesco, który skopiowaliśmy do katalogu z rawrite'em (np. *f4sdi.img*). Natomiast po ukazaniu się na ekranie komunikatu *'Enter target diskette drive:'* podać musimy literę, którą oznaczona jest u nas stacja dyskietek (czyli *a*). Pozostało nam już tylko wsunąć do stacji czystą sformatowaną

dyskietkę, wcisnąć ENTER i odczekać do zakończenia działania programu. Mamy już dyskietkę,
z której możemy wystartować naszego linuxa.

4.3 Konfiguracja Freesco dla SDI

Do pracy z SDI należy użyć specjalnie do tego celu zmodyfikowanego obrazu freesco (pliku
- *f4sdi.img*). Po przygotowaniu dykietki w sposób opisany w punkcie 4.2 uruchamiamy z niej
nasz komputer (jeżeli nie jest włączona w BIOSIE opcja botowania ze stacji dysków należy ją
włączyć). Gdy Freesco wystartuje logujemy się jako *root* (administrator). Początkowe hasło dla
administratora również brzmi: root. Po zalogowaniu wykonujemy kolejno poniższe czynności
(wybory zatwierdzaj wciskając ENTER):

[01] wpisz *setup* (aby wejść do setupu - miejsca konfiguracji Freesco),
[02] wybierz "a" (Advanced Settings),
[03] wybierz "3" (Add/Edit an ISP),
[04] (30) wpisz *sdi,*
[05] (31-35) zatwierdź wciskając sam ENTER,
[06] (37) wpisz swój adres IP nadany przez TPSA,
[07] wpisz adres półki na którą się logujesz (ew. pomiń),
[08] (39-40) zatwierdź wciskając ENTER,
[09] (R0) wpisz swój login dla usługi SDI,
[10] (R1) wpisz swoje hasło dla usługi SDI,
[11] wybierz "71" (Host/Domain),
[12] wpisz nazwę dla tego komputera,
[13] wpisz nazwę twojej domeny (nazwę - Otoczenia Sieciowego),
[14] wybierz "72" (1st network)
[15] (721) naciśnij ENTER,
[16] (724) wpisz adres IP serwera dla sieci wewnętrznaj (ew. ENTER),
[17] (725) wpisz maskę podsieci (ew. ENTER),
[18] (726) wciśnij ENTER,
[19] wybierz "30" (root),
[20] dwukrotnie wpisz nowe hasło dla root'a,
[21] wybierz "31" (control HTTP),
[22] dwukrotnie wpisz nowe hasło dla admina (przez www),
[23] wybierz "51" (COM port),
[24] wpisz do którego portu COM masz przyłączone SDI,
[25] wybierz "81" (1st card),
[26] wpisz port I/O dla karty sieciowej (jeżeli masz kartę PCI wpisz - 0x000),
[27] wpisz przerwanie IRQ (dla kart PCI wpisz - 0),
[28] wybierz "x" (back to main menu),
[29] wybierz "s" (save and exit),
[30] wpisz *reboot* (zresetuje się komputer).

4.4 Konfiguracja Freesco dla modemu.

Aby uruchomić Freesco na modemie należy użyć oryginalnego obrazu dystrybucji (*freesco-
0.2.7.zip*). Następnie uruchamiamy komputer z przygotowanej dyskietki i wykonujemy czynności (wszystkie zmiany zatwierdzamy klawiszem ENTER):

[01] logujemy się jako *root* (login: root, hasło: root),
[02] uruchamiamy konfigurację komendą *setup*,
[03] Wybieramy opcję "d" (Dialup line router),
[04] (*711) Hostname of this computer []? serwer* - nazwa dla tego komputera np. serwer,,
[05] (*712) Domain name []? inet* - nazwa lokalnej domeny (nie istniejąca w Internecie),
[06] (*50) Autoconfigure* - odpowiadamy "y" (yes) i czekamy aż wykryje modem,
[07] (*53) Modem init string []? ATZ* - wciskamy ENTER - string inicjalizayjny modemu,
[08] (8x) pyta, którą kartę sieciową chcesz skonfigurować, piszemy "1" i wciskamy ENTER,
[09] *(811) I/O port address ... []? 0x0* - zakres portów I/O (dla kart PCI - 0x0),
[10] *(812) IRQ line ... []? 0* - przerwanie karty sieciowej (dla kart PCI - 0),
[11] *(721) Interface name ... []? eth0* - nazwa interfejsu sieciowego - dajemy *eth0*,
[12] *(724) IP address ... []? 10.1.1.1* - adres IP jaki ma mieć ten interfejs sieciowy,
[13] *(725) Network mask []? 255.0.0.0* - maska podsieci,
[14] (726) IP range []? 10.1.1.2 10.1.1.20 - zakres lokalnych adresów IP (dla DHCP),
[15] *(411) Enable caching DNS server y/s/n []? s* - włączenie caching DNS (s-lokalnie),
[16] *(412) Enable DNS requests ... y/n []? n* - edycja konfiguracji DNS - dajemy "n" (no),
[17] *(421) Enable DHCP server y/s/n []? s* - włącznie servera DHCP (dajemy s - lokalnie),
[18] *(422) WINS address []?* - ustawienie adresu serwera WNIS (wciaskamy ENTER),
[19] *(423) Default-lease ... []? 604800 604800* - czas dzierżawy adresu IP (604800-7dni),
[20] *(424) Du you want ... []? n* - edycja statycznej tablicy numerów IP - wybieramy "n"),
[21] *(431) Enable public Http server y/s/n []? y* - włączenie serwera HTTP ("y" - na świat),
[22] (432) Public HTTP server IP port []? 80 - port dla servera www (wybieramy "80"),
[23] *(441) Enable time ... []? s* - włączenie serwera czasu i kontroli Freesco prez www,
[24] *(442) Control HTTP server IP port []? 82* - numer portu do administracji przez www,
[25] *(443) Host time server address ... []?* - adres synchronizacji serwera czasu (ENTER),
[26] *(444) Time offset to UTC []? +200* - strefa czasowa (+200 - letni, +100 - zimowy),
[27] *(451) Enable print server(s) y/s/n []? n* - włączenie serwera wydruku ("n" - nie),
[28] *(46) Enable tel*net server y/s/n []? s - zdalny dostęp poprzez telnet ("s" - lokalnie),
[29] *(14) Savers ... []?* - czas do wygaszania ekranu i uśpienia pracy dysków (ENTER),
[30] *(15) Swap file size in Megabytes ... []? 0* - wielkość pliku wymiany ("0" - wyłączony),
[31] *(13) Du you want to enable extra modules ... []? n* - dodatkowe moduły ("n" - nie),
[32] *(16) Log sizes in bytes ... []?* - maksymalna wielkość plików logów (dajemy ENTER),
[33] *(47) Du you want to export services y/n []? n* - forwardowanie portów na sieć loklną,
[34] *(480) Du you want to enable the DynDNS client []? n* - włączenie klienta DynDNS,
[35] *(30) ISP/connection name []? tpsa* - nazwa dla połączenia z usługodawcą sieciowym,
[36] (31) ISP phone numbers []? T0202122 - numer dostępowy do Internetu (T-tonowo),
[37] *(32) Keep up the ppp ... []?* - podtrzymanie połączenia po wysłaniu ostatniego pakietu . ("0" - według pliku filter.cfg, "1" - podtrzymuj zawsze),
[38] *(33) Primary DNS address []? 194.204.159.1* - adres podst. DNS'a (*dns.tpsa.pl*),
[39] *(34) Secondary DNS address []? 194.204.152.204* - adres pomocniczego DNS'a,
[40] *(35) ISP http proxy address []?* - adres serwera proxy naszego ISP (dajemy ENTER),
[41] *(36) Does you ISP ... []? y* - czy twój ISP przydziela dynamicznie adres IP ("y" - tak),
[42] *(39) Custom initialization.. []?* - dodatkowe konendy stringu inicjalizującego (ENTER),
[43] (40) Authentication method ... []? ppp - ustawienie metody autoryzacji (ENTER),
[44] (R0) Login name []? ppp - login (dla TPSA - "ppp"),
[45] (R1) Password []? ppp - hasło (dla TPSA - "ppp"),
[46] Changing password for root - zmiana hasła dla root'a (dwukrotnie nowe hasło),
[47] Changing password for user admin - zmiana hasła administratora przez www,
[48] wybieramy "s" w celu zapamiętania ustawień i resetujemy komputer komendą reboot,

4.5 Konfiguracja Freesco dla łącza z interfejsem RJ-45

Poniżej przedstawiona jest przykładowa konfiguracja dla ISP dostarczającego dostęp do Internetu
poprzez serwer proxy i modem podączony do karty sieciowej. Przyjmuję, że system jest
już zainstalowany. W następnym kroku należy skonfigurować karty sieciowe:

setup
2 (change advenced settings)
a (advenced settings)
81 (1st card)
881 0 (I/O port adress of 1st etherned card)
882 0 (IRQ line of 1st etherned card)
82 (2nd card)
821 0 (I/O port adress of 2nd etherned card)
822 0 (IRQ line of 2nd etherned card)
Teraz musimy skonfigurować sieci, sieć pierwsza:
72 (1st network)
720 n (Use DHCP client...)
721 eth0 (Interfece namefo 1st network)
724 xxx.xxx.xxx.xxx (IP adress of 1st network interface)
725 255.255.0.0 (network mask)
726 - (IP range)
- xxx.xxx.xxx.xxx - jest to adres IP taki jaki otrzymujemy do ISP poprzez DHCP,
- natomiast maska jest okreslona dla sieci klasy B a dokladniej dla sieci majacej
np. adres 192.168.xxx.xxx
Konfiguracja drugiej sieci:
73 (2nd network)
731 eth1 (Interfece namefo 2nd network)
732 xxx.xxx.yyy.yyy (P adress of 2nd network interface)
733 255.255.255.0 (network mask)
734 - (IP range)
- xxx.xxx.yyy.yyy - jest to adres IP bramy,
- natomiast maska jest okreslona dla sieci klasy C a dokladniej dla sieci majacej
np. adres 192.168.70.xxx
Dobrze aby 2 sieć była podsiecią sieci 1, ale nie jest to konieczne. Należy jeszcze ustawić serwer
proxy i bramę:
91 (Gateway/DNS/Proxy)
911 xxx.xxx.yyy.yyy (Host gateway)
912 (Primary DNS adress)
913 (Secondary DNS adress)
914 xxx.xxx.zzz.zzz[:p] (ISP http proxy adress)
- xxx.xxx.yyy.yyy - jest to adres IP drugiej karty sieciowej
- xxx.xxx.zzz.zzz - jest to adres serwera proxy
- [:p] - port serwera proxy

Ustawienie NAT:
11 y (Enable IP masquerade)
Użyte karty sieciowe są PnP dlatego zarówno IRQ jak i I/O ustawione są na 0. Można ewentualnie
przydzielić IRQ na stałe, np. dla pierwszej karty 10 a dla drugiej 11. W przypadku, gdy adres IP od providera jest przydzielany dynamicznie należy włączyć odpowiednią opcję w
setupie Freesco (punkt 36. Does your ISP give you a dynamic IP address []? dajemy 'y').
Autor: Rywal (gilmar@poczta.fm)
4.6 Konfiguracja serwera czasu.
Time server to program synchronizujący zegar naszego serwera z datą i czasem ustawionym
na odpowiednim serwerze czasu w sieci (jest on synchronizowany poprzez Internet). Time server jest stndardowo zainstalowany we Freesco, wystarczy go tylko uaktywnić (setup, 44).
(441) enable time server - wybierz s
(442) port [82] - nie trzeba zmieniać
(443) Host Time server address - 149.156.4.11 (ten jest najbliżej)
(444) Time offset - +0100
Z powodu braku zainteresowania "polskim" formatem daty, autorzy pominęli to co nas interesuje
(rr.mm.dd) musimy więc to poprawić na serwerze. Należy wyedytować plik: *edit /wwa/time*
Bezpośrednio za tymi trzema liniami:
```
case "$QUERY_STRING" in
dmy) W "%d-%m-%Y";;
mdy) W "%m-%d-%Y";;
```
należy dopisać:
```
ymd) W "%Y-%m-%d";;
```
i zapisać dokonane zmiany. Klientem usługi pod windowsa jest program, który można pobrać
z Polskiej Strony Freesco (http://www.freesco.arx.pl) z działu download (date-w32.zip).
Aby zsynchronizować swoją datę z serwerem należy uruchomić:
```
netdate 10.1.1.1 82 ymd
```

4.7 Konfiguracja serwera DHCP+ARP
Odpowiednia konfiguracja pozwala na to aby użytkownicy na swoich komputerach nic nie robili
jeśli chodzi o konfigurowanie sieci (TCP/IP). Kiedy DHCP działa poprawnie, użytkownik nie
musi mozolnie wpisywać wszystkich parametrów sieci jak numer IP, maska podsieci, brama
etc. na przykład po reinstalacji systemu. Identyfikacja użytkownika następuje po numerze
MAC karty sieciowej - który to numer jest unikatowym numerem przydzielonym każdej karcie.
Oczywiście cała bajera byłaby nie na miejscu gdyby nasze kochane FREESCO nie umożliwiało
opcji włączenia serwera DHCP.
Pakiet ARP natomiast dopilnuje, aby użytkownicy, którym został przypisany dany numer ip nie
mogli go zmienić. Pakiet ARP analizuje numer MAC karty sieciowej i na jego podstawie udziela,
lub zabrania na dostęp danemu użytkownikowi.
4.7.1 Konfiguracja DHCP
Zanim zaczniecie jednak grzebać na serwerze potrzebne będą numery wszystkich kart sieciowych.
Jak je zdobyć? Pod windą kiedy już macie zainstalowaną kartę należy uruchomić plik winipcfg.exe z katalogu \WINDOWS. Tam znajdziecie numer karty którego struktura będzie
wyglądać mniej więcej tak:
00:cd:41:09:b1:c0
Teraz już macie wszystko przejdźcie więc do konfiguracji servera. Załóżmy że do SETUP'u
każdy z was już potrafi się dopchać (ale przypomnę: login: root, hasło, wpisujemy setup ENTER,
ENTER, wpisujemy a ENTER) Musimy wykonać więc kolejno czynności:

wpisz 72 i zatwierdź klawiszem ENTER,
(721) podaj numer numer interfejsu sieciowego,
(722) podaj IP twojego servera (np. 10.1.1.1),
(723) maska podsieci dla twojej sieci (np. 255.0.0.0),
(724) IP range - pula adresów z której będą one przydzielane komputerom w sieci,
(np. mam w sieci cztery komputery + serwer - 10.1.1.1, więc w IP range
wpisałem 10.1.1.2 10.1.1.5 bo mam 4 kompy w sieci i więcej nie trzeba),
wpisz 42 i zatwierdź klawiszem ENTER,
(421) wpisz s i zatwierdź klawiszem ENTER,
(422) wciśnij ENTER,
(423) wciśnij ENTER,
(424) wpisz y i zatwierdź klawiszem ENTER,
jeszcze dwa razy wciśnij ENTER,

Ostatnie pytanie dotyczyło edycji pliku dhcpd.conf. Wybraliśmy y (yes). Teraz więc musimy
wpisać tu kolejno userów sieci w podanej niżej stukturze:

```
host win98{
fixed-address 10.1.1.2
hardware ethernet 00:c0:de:41:c9:61
}
```

gdzie fixed-address to IP jakie ma otrzymać komputer o numerze karty sieciowej która jest
zidentyfikowana poprzez parametr hardware ethernet czyli dla komputera o numerze karty
sieciowej 00:c0:de:41:c9:61 zostanie przydielony adres 10.1.1.2
Tak robimy dla wszyskich komputerów w sieci przydzielając kolejne numery ip kolejnym komputerom.
Poz zakończeniu wciskamy Alt+X i dajemy s (czyli save). Restart servera komendą reboot. Oczywiście teraz w komputerach klienckich w ustwieniach TCP/IP wszystkie wpisy
usuwamy jeżeli wcześniej ustawiliśmy je na "sztywno" m.in. musimy ustwić opcje - "Automatycznie
pobierz numer IP". Od tego momentu komputer przy uruchamiania automatycznie będzię szukał servera DHCP jeżeli znajdzie wyśle informacje o swoim numerze karty sieciowej.
Jeżeli server odnajdzie ten numer w pliku konfiguracyjnym przydzieli mu IP i inne niezbędne
dane. Prawde że fajnie ;)

4.7.2 Konfiguracja ARP

ARP to oprogramowanie utrudniające podszywanie się komuś z sieci pod nasz IP w trakcie
naszej nieobecności. Porównuje ono adres IP komutera z adresem MAC karty sieciowej spod
której dany IP jest używany i jeśli identycznego zapisu nie ma w swoim zapisie odrzuca dany
komputer z dostępu do serwera.
Po zainstalowaniu ARP należy wyedytować plik przypisujący adres IP do konkretnej karty
sieciowej. Plik ten to /mnt/router/packages/arp/hosts.arp. Jego struktura jest dość prosta:
najpierw podaje się adres IP a następnie adres MAC karty sieciowej. Dla przykładu:
192.168.0.1 00:00:E8:62:63:8E i tak po kolei z każdym adresem z sieci.
Linijki zaczynające sie na # trkatowane są jako komentarz. Aby uruchomić ARP zaraz po zainstalowaniu
bez restartu komputera wystarczy wpisać: "rc_arp start". W przypadku gdy administrujesz
zdalnie najpierw upewnij sie dokładnie czy poprawnie wpisałeś adresy a szczególnie swój inaczej momentalnie po uruchomieniu tracisz dostęp do komputera. Wszelkie zmiany w
pliku hosts.arp można zatwierdzić komendą: "rc_arp restart."

4.8 Konfiguracja serwera DNS (BIND8)

Na początku, zanim Internet osiągnął swoje rozmiary, a właściwie zanim jeszcze nazwano go
Internetem, każdy komputer musiał posiadać dane tylko o niektórych komputerach w Sieci;
lista ważnych komputerów była umieszczana w pliku hosts.txt. Co więcej, plik ten był tworzony
i utrzymywany przez jedną, centralną organizację o nazwie InterNIC, udostępniającą ten
plik innym komputerom. Administratorzy węzłów musieli wysyłać pocztą informacje o zmianach
do organizacji InterNIC, która odpowiadała za uaktualnienie informacji. W miarę upływu
czasu poszczególne komputery poszczególne komputery pobierały uaktualnioną wersję pliku i
w ten sposób informacje o zmianach rozchodziły się w Sieci.
Takie rozwiązanie rodzi jednak problemy - przede wszystkim nie jest skalowalne. W miarę rozrastania
się sieci Internet rosła wielkość pliku i efektywne zarządzanie zawartymi w nim informacjami
stało się niemożliwe. Twórcy sieci przeanalizowali wówczas problem i opracowali plan nowego, lepszego systemu, radzącego sobie z ogromną liczbą komputerów. Nie posiadał on
wąskich gardeł w postaci pojedynczego administratora czy punktu dystrybucyjnego (jak miało
to miejsce w przypadku systemu kontrolowanego przez InterNIC), pozwalając jednocześnie na
dystrybucję informacji o zmianach w rozsądnym czasie. Takim właśnie systemem jest DNS.
DNS to w zasadzie prosta, rozproszona baza danych, dająca możliwość delegowania odpowiedzialności (administracji i dystrybucji) oraz posiadająca bardzo ważną własność -
możliwość buforowania odpowiedzi na zapytania; te cechy powodują, że świetnie sprawdza
się ona nawet w dzisiejszym Internecie.
Program BIND (ang. Berkley Internet Name Deamon) jest właśnie implementacją takiej
rozproszonej bazy danych. Przez wiele lat BIND w wersji 4. był jedyną implementacją, ale
w końcu się zestarzał i został zastąpiony przez BIND 8. BIND 4 miał również sporo problemów
z bezpieczeństwem - zostały one poprawione w wersji 8. Wersja 8 jest obecnie wersją zalecaną, szczególnie w przypadku węzłów, w których istotne są zagadnienia związane z
bezpieczeństwem.

Instalujemy BIND 8

Pakiet instalujemy ze strony autora:
installpkg http://freesco.docnielsen.dk/bind8

lub z poniższych adresów:
installpkg http://mkgnet.one.pl/freesco/bind8
installpkg http://www.freesco.arx.pl/pakiety/bind8

Konfiguracja programu BIND

Po zainstalowaniu programu BIND dokonujemy jego lokalnej konfiguracji. Program rezydentny,
działający jako serwer nazw, nazywa się named a jego konfiguracja jest zapisana w pliku
/mnt/router/packages/bind8/etc/named.conf. W tym pliku znajdują się podstawowe parametry tego programu i wykaz stref, który nasz serwer ma obsługiwać, oraz plików, w których
są one zapisane.
Najprostsza i najłatwiejsza w administrowaniu konfiguracja serwera nazw - serwer buforujący
- działa we Freesco po zainstalowaniu pakietu. Przedstawiona dalej konfiguracja serwera nazw
jest bardziej rozbudowana i charakteryzuje się:
- wprowadzeniem dla każdego interfejsu niezależnych plików stref co pozwala na ukrywanie
ważnych z punktu bezpieczeństwa informacji dotyczących naszej sieci i serwera;
- wprowadzeniem własnych kanałów dla generowania komunikatów diagnostycznych przez
serwer nazw co odciąża systemowego sysloga i umożliwia odtworzenie logów serwera sprzed
'padnięcia';
- wprowadzeniem list kontroli dostępu i transferu stref dzięki czemu znacznie podnosi się
bezpieczeństwo serwera;

Konfiguracja stref

Najpierw zaczniemy od konfiguracji plików stref. Pliki te standardowo umieszczone są w katalogu
/mnt/router/packages/bind8/zones. W nazewnictwie plików stref można spotkać kilka konwencji, ja przyjąłem najbardziej popularną, czyli nazwa pliku pokrywa się z nazwą strefy
(sieci), której plik dotyczy.
Jako pierwszą skonfigurujemy strefę, która dotyczyć będzie naszej domeny internetowej, np.
mojlan.one.pl. Zatem w katalogu zones tworzymy plik o nazwie *mojlan.one.pl*:

```
;
;mojlan.one.pl zone
;
$TTL 804800 ;7 dni
$ORIGIN mojlan.one.pl.
@ IN SOA ns.mojlan.one.pl. root.mojlan.one.pl. (
2002021800 ; Serial
86400 ; Refresh 24h
7200 ; Retry 2h
3600000 ; Expire 1000h
86400 ; Minimum TTL 24h
)
;
```

Pierwszy wiersz definicji rekordu SOA (wiersz 6) zawiera dwie istotne informacje. Pierwsza
z nich to nazwa serwera obsługującego strefę, czyli ns.mojlan.one.pl. Powinna to być nazwa
serwera nazw, a nie samej strefy, chyba że nazwy te się pokrywają. Druga informacja to adres
e-mailowy osoby odpowiedzialnej za utrzymanie strefy, w tym przykładzie root.mojlan.one.pl.
Ten wpis oznacza adres root@mojlan.one.pl (pierwsza kropka jest zastępowana znakiem @).
Kolejne wiersze w pliku zawierają kilka innych, ważnych parametrów. Numer seryjny - Serial
- musi być zwiększany przy każdej modyfikacji pliku. Rozpowszechnioną i wygodną konwencją
jest nadawanie strefom numerów seryjnych w postaci YYYYMMDDNN - osiem pierwszych cyfr
oznacza datę modyfikacji, a dwie ostatnie - numer modyfikacji danego dnia. W parametrze
Refresh ustawiamy czas, po którym wszystkie serwery podrzędne mają obowiązek sprawdzić,
czy dane w serwerze nadrzędnym nie zostały zmodyfikowane. Czas ponowienia próby - Retry
- ma znaczenie jedynie w przypadku, gdy serwer podrzędny nie będzie mógł skontaktować
się z serwerem nadrzędnym po upływie okresu odświeżania. Parametr Expire definiuje okres
ważności strefy. Parametr Minimum TTL określa czas buforowania negatywnych odpowiedzi,
czyli czas, przez jaki serwer nazw pamięta, że dana nazwa domenowa nie istnieje. Czas buforowania
wszystkich rekordów w strefie jest natomiast określony wartością parametru $TTL.

```
IN NS ns
IN NS ns.innylan.one.pl.
IN MX 10 mail
```

W wierszu 14 znajduje się kolejna ważna informacja - rekord NS dla strefy. Wymagane jest
istnienie przynajmniej jednego takiego rekordu. W tym przykładzie są wprowadzone dane
o dwóch serwerach nazw - zaprzyjaźniona sieć utrzyma dla nas zapasowy serwer nazw.
Jeśli nie mamy zapasowego serwera DNS to po prostu wiersz 15 pomijamy - secDNS'a możemy dopisać później. Nie mniej jednak brak zapasowego serwera nazw uniemożliwi
nam rejestrację domeny w NASK'u. Nie można w rekordach NS podawać od razu adresów
IP - należy podać nazwy domenowe, a następnie wprowadzić rekordy A zawierające odpowiednie
adresy. Adres komputera o nazwie ns.mojlan.one.pl znajduje się w wierszu 18. W pliku strefy nie znajduje się natomiast adres serwera ns.innylan.one.pl, ponieważ należy on
do innej strefy i trzeba go znaleźć w odmienny sposób. Wiersz 16 to rekord MX, określający
serwery poczty obsługujące daną domenę, czyli mojlan.one.pl. Rekord ten wymaga dwóch
pól danych: pierwsze z nich określa priorytet, drugie - nazwę serwera poczty. Program pocztowy
będzie próbował dostarczyć pocztę za pomocą serwera o najniższym priorytecie - jeśli

mu się to nie uda, zostanie podjęta próba wysłania za pośrednictwem kolejnych serwerów.
Korzystanie z zapasowych serwerów poczty nie jest tak bardzo istotne, gdyż serwer poczty,
który próbuje wysłać pocztę, w przypadku niepowodzenia ponawia próby przez kilka dni,
zanim się podda - zwykle są to trzy dni.

```
;serwer nazw
ns IN A aaa.aaa.aaa.aaa
```

W wierszu 18 definiujemy adres IP komputera będącego naszym serwerem nazw. W miejsce
aaa.aaa.aaa.aaa należy wpisać IP jakie przydzieliła TP S.A. dla naszego SDI.

```
;serwer poczty
mail IN A aaa.aaa.aaa.aaa
IN MX 10 mail
```

Kolejny rekord A (wiersz 20) opisuje komputer mail.mojlan.one.pl, podając taki sam adres
IP. Ten serwer poczty posiada również rekord MX, na wypadek gdyby ktoś próbował wysłać
pocztę do użytkownika w systemie *@mail.mojlan.one.pl.*

```
;serwer www
www IN A aaa.aaa.aaa.aaa
IN MX 10 mail
@ IN A aaa.aaa.aaa.aaa
```

Dzięki powyższym rekordom stronę WWW naszej sieci będzie można zobaczyć zarówno
wpisując adres *http://www.mojlan.one.pl* jak i *http://mojlan.one.pl*. Protokół HTTP wymaga
po prostu rekordu A serwera z którym ma się połączyć, więc taki rekord podaliśmy. Podobnie
wygląda sprawa w przypadku serwera FTP. Dla serwera WWW dodano również rekord MX
(wiersz 24) na wypadek gdyby ktoś chciał wysłać maila na adres *webmaster@www.mojlan.o*
ne.pl.

```
;serwer ftp
ftp IN A aaa.aaa.aaa.aaa
```

W pliku tym można również podać informacje dotyczące hostów działających w sieci lokalnej
jednak z punktu bezpieczeństwa nie zaleca się tego robić.
Teraz skonfigurujemy strefę domeny wewnętrznej, np. lan. Jaki jest sens tworzenia tej strefy?
Przede wszystkim upraszcza się korzystanie z usług dostępnych w naszej sieci, np. stronę
WWW naszej sieci można wywołać wpisując adres http://www.lan lub jeszcze krócej http://
lan. Poza tym można ukryć w strefie internetowej niektóre usługi (np. serwer FTP), natomiast
dla użytkowników naszej sieci będą one dostępne. Kolejną zaletą strefy domeny wewnętrznej
jest opisanie wszystkich maszyn pracujących w sieci, dzięki czemu można wyszukiwać komputer
po nazwie a nie tylko po IP.

A więc w katalogu zones tworzymy kolejny plik o nazwie lan o postaci:

```
;
;lan zone
;
$TTL 804800 ;7 dni
$ORIGIN lan.
@ IN SOA ns.lan. root.lan. (
2002021800 ; Serial
86400 ; Refresh 24h
7200 ; Retry 2h
3600000 ; Expire 1000h
86400 ; Minimum TTL 24h
)
;
IN NS ns
IN MX 10 mail
```

Tu widać pierwszą różnicę w stosunku do pliku *mojlan.one.pl.* Dla domeny wewnętrznej mamy
tylko jeden rekord NS. Tworzenie zapasowego serwera nazw dla domeny wewnętrznej ma
sens w przypadku bardzo rozbudowanych sieci mających kilkadziesiąt lub kilkaset hostów.

```
;serwer nazw
ns IN A 192.168.1.1
;serwer poczty
mail IN A 192.168.1.1
IN MX 10 mail
HINFO PC Linux
```

Rekord HINFO przekazuje informacje o komputerze. Wymaga on dwóch pól danych: pierwsze
z nich to informacja o procesorze, drugie - o systemie operacyjnym. Rekord HINFO może
potencjalnie stanowić lukę w bezpieczeństwie dostarczając napastnikowi informacji o typie
systemu operacyjnego działającego na danym komputerze, co pozwoliłoby przejść od razu
do prób włamania sposobami odpowiednimi dla danego systemu. Dlatego rekord HINFO nie
pojawił się w pliku strefy domeny internetowej.

```
;serwer www
www IN A 192.168.1.1
IN MX 10 mail
@ IN A 192.168.1.1
;serwer ftp
ftp IN A 192.168.1.1
;siec wewnetrzna
router IN A 192.168.1.1
host1 IN A 192.168.1.2
host2 IN A 192.168.1.3
host3 IN A 192.168.1.4
...
```

Dla strefy domeny wewnętrznej musimy jeszcze utworzyć strefę odwrotną. Tworzymy więc
kolejny plik w katalogu zones o nazwie 192.168.1.

```
;
```

```
;1.168.192.in-addr.arpa zone
;
$TTL 804800 ;7 dni
$ORIGIN 1.168.192.in-addr.arpa.
@ IN SOA ns.lan. root.lan. (
2002021800 ; Serial
86400 ; Refresh 24h
7200 ; Retry 2h
3600000 ; Expire 1000h
86400 ; Minimum TTL 24h
)
IN NS ns.lan.
```

Bardzo ważną rzeczą jest wpisywanie pełnych nazw domenowych, czyli ogólnie mówiąc nie wolno zapominać o kropkach na końcu nazwy domenowej. Jest to najczęstszy błąd popełniany przy tworzeniu strefy odwrotnej.

```
;dzialajace serwery
1 IN PTR ns.lan.
1 IN PTR mail.lan.
1 IN PTR www.lan.
1 IN PTR ftp.lan.
;siec wewnetrzna
1 IN PTR router.lan.
2 IN PTR host1.lan.
3 IN PTR host2.lan.
4 IN PTR host3.lan.
...
```

Na koniec pozostało utworzenie strefy dla interfejsu pętli zwrotnej (lo0). Większość opracowań na temat konfiguracji serwera nazw (np. DNS-HOWTO) wprowadza rekord A opisujący komputer localhost w pliku strefy domeny internetowej (ewentualnie wewnętrznej). Taki zapis jest oczywiście poprawny, nie mniej jednak komputer localhost o adresie IP 127.0.0.1 reprezentuje odrębną sieć, dlatego niektórzy znawcy tematu proponują tworzenie odrębnego pliku strefy dla tej sieci. W tym przykładzie została przyjęta taka właśnie koncepcja. Zatem tworzymy kolejny plik w katalogu zones o nazwie localhost, którego postać jest następująca:

```
;
;localhost zone
;
$TTL 804800 ;7 dni
$ORIGIN localhost.
@ IN SOA localhost. root.localhost. (
2002021800 ; Serial
86400 ; Refresh 24h
7200 ; Retry 2h
3600000 ; Expire 1000h
86400 ; Minimum TTL 24h
)
;
IN NS localhost.
IN A 127.0.0.1
```

Ostatni plik strefy jaki należy utworzyć to strefa odwrotna do localhost. Tworzymy plik 127.0.0 w katalogu zones o postaci:

```
;
;0.0.127.in-addr.arpa zone
;
$TTL 804800 ;7 dni
$ORIGIN 0.0.127.in-addr.arpa.
@ IN SOA localhost. root.localhost. (
2002021800 ; Serial
86400 ; Refresh 24h
7200 ; Retry 2h
3600000 ; Expire 1000h
86400 ; Minimum TTL 24h
)
;
IN NS localhost.
1 IN PTR localhost.
```

Na koniec ważna uwaga: w plikach stref dozwolonym znakiem komentarza jest wyłącznie znak średnika (;). Wprowadzenie innego znaku np. // lub # spowoduje, że named zgłosi błędy składni i odrzuci całą strefę.

Konfiguracja named'a

Skoro mamy już skonfigurowane pliki stref pozostaje skonfigurować program rezydentny serwera nazw. Jak już wcześniej zostało wspomniane plik konfiguracyjny znajduje się w katalogu */mnt/router/packages/bind8/etc* i nazywa się *named.conf*. Plik ten ma ściśle określoną składnię, której trzeba przestrzegać. Najmniejszy błąd składniowy powoduje odrzucenie pliku konfiguracyjnego.

Plik *named.conf* można podzielić na kilka sekcji. Najważniejsze z nich to opcje globalne dla serwera nazw oraz konfiguracja stref. Dodatkowymi sekcjami, które możemy wykorzystać to listy dostępu oraz diagnostyka named'a.

Przystępujemy zatem do edycji named.conf:

```
// BIND 8 config file
// Konfiguracja serwera DNS dla domeny mojlan.one.pl
// listy dostepow
acl bogusnet {
0.0.0.0/8; // brak adresu
1.0.0.0/8; // adresy zarezerwowane przez IANA
2.0.0.0/8; // często wykorzystywane przy atakach
192.0.2.0/24; // adresy testowe
224.0.0.0/3; // adresy rozgloszeniowe
// niewykorzystywane adresy klasy C w sieci mojlan
10.0.0.0/8;
176.16.0.0/12;
};
acl our-nets { 192.168.1.0/24; }; // nasza siec
```

```
acl our-sec { // oni są moimi secondary
xxx.xxx.xxx.xxx/32;
};
```

Kilkukrotne wyliczanie sieci w pliku konfiguracyjnym jest męczące i może być przyczyną błędów. Z tego powodu w programie BIND można korzystać z list dostępu (acl), których potem możemy używać przy ograniczaniu czy przyznawaniu dostępu. Lista acl może zawierać dowolną liczbę sieci i pojedynczych komputerów. W tym przykładzie występują trzy listy dostępu: *bogusnet, our-nets i our-sec*, określających kolejno listę podejrzanych adresów, które będą kierowane do 'czarnej dziury', listę adresów należących do naszej sieci oraz listę adresów IP zapasowych serwerów nazw (za xxx.xxx.xxx.xxx należy wpisać IP serwera, który będzie serwerem zapasowym dla naszej domeny *mojlan.one.pl*).

```
// diagnostyka BIND'a
logging {
channel main-log {
file "var/log/main.log" versions 3 size 4M;
print-time yes;
print-category yes;
print-severity yes;
};
```

Instrukcją channel definiujemy kanał dla komunikatów generowanych przez serwer nazw. Każda definicja kanału musi zawierać informację gdzie mają być zapisywane przesyłane przez kanał dane oraz jakie informacje dodatkowe mają być z tym komunikatem przesyłane. Opcja file określa nazwę pliku do jakiego będą przesyłane komunikaty. Parametr version ile powstanie plików z logami w wyniku ich rotacji, zaś size określa rozmiar tego pliku. Pozostałe opcje definiują, że z komunikatem serwera nazw ma pojawić się data i czas komunikatu, jego kategoria oraz poziom ważności.

```
channel security-log {
file "var/log/security.log" versions 3 size 2M;
print-time yes;
print-severity yes;
};
channel query-log {
file "var/log/query.log" versions 3 size 2M;
print-time yes;
print-severity yes;
};
channel statistic-log {
file "var/log/statistic.log" versions 3 size 1M;
print-time yes;
print-severity yes;
};
channel panic-log {
file "var/log/panic.log" versions 3 size 1M;
print-time yes;
print-severity yes;
};
category default { main-log; };
category security { security-log; main-log; };
category queries { query-log; };
category statistics { statistic-log; };
category db { statistic-log; };
category response-checks { query-log; main-log; };
category panic { panic-log; main-log; };
};
```

Poszczególne kategorie komunikatów przesyłać można do zdefiniowanych wcześniej kanałów przy pomocy instrukcji category. Jak widać domyślnym kanałem dla komunikatów o kategoriach niezdefiniowanych instrukcją category jest kanał *main-log*. Natomiast komunikaty związane z otrzymanymi zapytaniami przesyłane są do kanału *query-log*.

Oczywiście brak sekcji logging nie powoduję, że BIND nie będzie generował żadnych komunikatów. W takim przypadku wszystkie komunikaty named'a powędrują do systemowego sysloga.

```
// opcje globalne dla serwera DNS
options {
// sciezki dostepu
version "I'm not telling. Who are you?";
directory "/mnt/router/packages/bind8/";
named-xfer "bin/named-xfer";
pid-file "var/named.pid";
dump-file "var/named_dump.db";
// opcje kontroli dostepu i transferu stref
allow-query { localhost; our-nets; };
allow-recursion { localhost; our-nets; };
allow-transfer { our-sec; }; // transfer strefy mogą tylko zadąć
twoje secDNS
blackhole { bogusnet; }; // czarna dziura dla kompów z bogusnet
query-source port 53;
listen-on {
aaa.aaa.aaa.aaa; // zewnętrzny adres IP serwera
192.168.1.1; // wewnętrzny adres IP serwera
127.0.0.1; // interfejs localhost
};
// opcje logiczne
recursion yes; // zezwalamy na obsługę zapytań rekursywnych
check-names master fail;
check-names slave warn;
check-names response ignore;
// topologia
topology { localhost; localnets; };
// czestotliowsc zadan okresowych
cleaning-interval 120; // czyszczenie pamięci buforowej co
2h
interface-interval 0; // skan interfejsów tylko na starcie
statistics-interval 360; // statystyki co 6h
};
```

```
// konfiguracja stref
zone "." IN {
type hint;
file "zones/named.root";
};
zone "mojlan.one.pl" IN { // strefa zewnętrzna
type master;
file "zones/mojlan.one.pl";
allow-update { none; };
allow-query { any; };
notify yes;
};
zone "localhost" IN { // strefa lokalnego hosta
type master;
file "zones/localhost";
allow-update { none; };
allow-transfer { none; };
};
zone "0.0.127.in-addr.arpa" IN { // rev dla lokalnego hosta
type master;
file "zones/127.0.0";
allow-update { none; };
allow-transfer { none; };
};
zone "lan" IN { // strefa wewnętrzna
type master;
file "zones/lan";
allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN { // rev dla strefy wewnętrznej
type master;
file "zones/192.168.1";
allow-update { none; };
};
```

Jeżeli nasz serwer nazw ma pełnić również funkcję zapasowego serwera dla innej domeny np.
domeny naszej zaprzyjaźnionej sieci *innylan.one.pl* konieczne jest dopisanie w *named.conf* następującej pozycji:

```
zone "innylan.one.pl" IN { // strefa prosta serwera zapasowego dla
domeny innylan.one.pl
type slave;
file "zones/innylan.one.pl";
masters {
sss.sss.sss.sss;
};
};
```

Instrukcja *masters* pozwala określić, które serwery są serwerami nadrzędnymi (w miejsce
sss.sss.sss.sss wpisujemy IP serwera nadrzędnego). Nazwy stref powinny być takie same jak w przypadku serwera nadrzędnego - w końcu są to definicje tych samych stref. Plik strefy
zapisywany jest w katalogu zones (można tu podać inny katalog, wtedy będziemy mieć osobno
pliki stref serwera naszej domeny *mojlan.one.pl* i osobno pliki stref serwera domeny *innylan.one.pl* dla której jesteśmy serwerem zapasowym).

Konfiguracja Freesco i uruchomienie BIND'a

Pozostaje jeszcze uzupełnienie informacji dotyczących nazwy hosta i domeny w setup'ie
naszego Freesco.
Host/Domain - pozycja 71
711 Hostname of this computer [router]? - wpisujemy router
712 Domain name [inet]? - wpisujemy mojlan.one.pl
Informacje dotyczące uruchomienia usługi serwera nazw (pozycja 41) skrypt instalacyjny
BIND8 uzupełni za nas. Po wprowadzeniu wszystkich zmian, pozostaje tylko zrestartować serwer
DNS co wykonuje się komendą: *rc_bind8 restart* lub zrebootować Freesco (w przypadku gdy dokonane zostały zmiany w setup'ie).

Informacje:

Dokumentacja BIND'a (http://www.isc.org/products/BIND/bind8.html)
DNS-HOWTO (http://www.jtz.org.pl/Html/DNS-HOWTO.pl.html)

Domeny:

NASK - domeny płatne .pl, com.pl, org.pl, net.pl, i inne (http://www.dns.pl)
ONE.PL - domeny darmowe one.pl (http://www.one.pl)

Autor: Maciej Kuśmierczak (mkusmierczak@mkgnet.one.pl)

5. FREESCO NA DYSKU TWARDYM

5.1 Po co Freesco na HDD?
Freesco umożliwia przeniesienie na dysk twardy. Jest wiele zalet takiego rozwiązania. Najważniejsza to to, że możemy kożystać z dodatkowych pakietów dla których na dyskietce
z pewanością zabrakłoby miejsca. Na dysku twardym możemy umieścić również serwer FTP,
rozbudowany serwis www, oraz wiele innych ciekawych rozwiązań. Ważne jest również, to, że
po przeniesieniu Freesco na dysk twardy w całości system startuje znacznie szybciej.
5.2 Przenoszenie Freesco na dysk twardy.
Najwpierw należy przygotować sformatowany w systemie FAT (w dosie) dysk twardy. Następnie należy przygotować sobie DOS'ową dyskietkę startową, albo przenieść system z
dyskietki DOS na dysk twardy.
Po uruchomieniu Freesco z dyskietki i zalogowaniu się jako *root* wydajemy komendę *move2hdd,* a następnie wybieramy opcję "c" (Clean install). Po chwili nasze Freesco znajduje
się już na dysku twardym. Teraz resetujemy serwer komendą *reboot*, podczas startu wyjmujemy
dyskietkę z Freesco i jeżeli nie mamy systemu na HDD to wkładamy do stacji odpowiednio
przygotowaną dyskietkę startową DOS.
5.3 Dyskietka startowa DOS ze skanowaniem dysku.
Formatujemy dyskietkę poleceniem *format a: /s,* kopiujemy na nią pliki *scandisk.exe* i *scandisk.ini*, oraz tworzymy plik *autoexec.bat*, który ma wyglądać tak:

```
a:\scandisk.exe /all /nosave /autofix /nosummary
c:\router.bat
```

Natomiast plik scandisk.ini ma mieć takie wpisy:

```
[ENVIRONMENT]
Display = Auto
Mouse = On
```

ScanTimeOut = Off
NumPasses = 1
LabelCheck = Off
LfnCheck = On
SpaceCheck = Off
Mount = Never
Boot_Sector = Fix
FSInfo_Sector = Fix
Invalid_MDFAT = Fix
DS_Crosslinks = Fix
DS_LostClust = Fix
DS_Signatures = Fix
Mismatch_FAT = Fix
Bad_Clusters = Fix
Bad_Entries = Quit
LostClust = Delete
[CUSTOM]
DriveSummary = Off
AllSummary = Off
Surface = Never
CheckHost = Never
SaveLog = Off
Undo = Never
DS_Header = Fix
FAT_Media = Fix
Okay_Entries = Fix
Bad_Chain = Fix
Crosslinks = Fix

5.4 Uruchamianie Freesco z dysku bez MS-DOS-a.

Aby zainstalować Freesco 0.2.7 na dysku twardym bez korzystania z plików startowych MS
DOS-a należy upewnić się, że nasza partycja posiada system plików FAT-12 lub FAT-16 (FAT-32
nie jest obsługiwany). Następnie należy pobrać plik *syslinux.gz*
(http://www.freesco.arx.pl/
download/freesco/syslinux.gz) i zapisać go na dysku z Freesco w katalogu a:\router\
Teraz musisz uruchomić Freesco z dyskietki i skopiować plik syslinux.gz do katalogu /tmp
komendą: *cp /mnt/router/syslinux.gz /tmp/syslinux.gz*
Kolejnym krokiem będzie rozpakowanie archiwum i nadanie atrybutu wykonywalności:
zcat </tmp/syslinux.gz >/tmp/syslinux
chmod a+x /tmp/syslinux
Przenosimy teraz nasz router na dysk twardy komendą: *mowe2hdd*, a następnie montujemy
tę partycję poleceniem: *mount -t umsdos /dev/hda1 /hd.*
Następnie kopiujemy ramdisk i jądro:
cp /hd/router/ramdisk /hd
cp /hd/router/kernel /hd
Oraz tworzymy nowy plik konfiguracyjny:
cat /mnt/syslinux.cfg | sed s/fd0/hda1/g > /hd/syslinux.cfg
Odmontowujemy partycję: *umount /hd* i instalujemy syslinux-a: *syslinux /dev/hda1*.
Ostatnie co musimy zrobić, to zatrzymać router komendą *halt* i uruchomić ponownie już z
dysku twardego.

5.5 Instalacja dodatkowych pakietów.

Aby doinstalować do Freesco jakiś dodatkowy pakiet wydajemy z konsoli Freesco komendę:
*installpkg adres/pakie*t np. komendą *installpkg http://www.freesco.arx.pl/pakiety/top* zainstalujemy na serwerze pakiet *top* (ststystyki serwera). Oczewiście pakiety możemy instalować z dowolnego serwera (zarówno http jak i ftp) na którym one się zanjdują.
Aby odinstalować pakiet musimy wydać komendę *removepkg nazwa_pakietu*, analogicznie do
przykładu powyżej komenda *removepkg top* usunie nam z serwera pakiet *top.*
Aby uzyskać listę pakietów dostępnych na danym serwerze musimy wydać komendę: *listpkg adres_serwera,* np. komenda *listpkg http://www.freesco.arx.pl/pakiety/* wyświetli nam listę pakietów dostępnych na tym serwerze. Instalację pakietów możemy przeprowadzać
również z serwera http uruchomionego w sieci lokalnej, na którym udostępnimy pakiety dla
Freesco. Pakiety te należy najwpierw pobrać z sieci www.

5.6 Lista serwerów/mirrorów z pakietami dla Freesco.

Najpopularniejszym i zarazem oficjalnym serwerem z pakietami dla Freesco jest serwer:
http://www.freescosoft.com/, na stronach tego serwera znajdziemy linki do wielu jego mirrorów.
Oto lista serwerów, z których możemy instalować wybrane pakiety:
Serwery z pakietami w Polsce:
http://www.freesco.arx.pl/pakiety/ - serwer Oficjalnej Polskiej Strony Freesco,
http://www.freesco.arx.pl/pakiety/ - archiwum z większą ilością pakietów,
http://www.cinas.mine.nu/freesco/ - archiwum z pakietami cinasa,
Serwery z pakietami za granicą:
http://freesco.docnielsen.dk/ - Doc Nielsen's Freesco Package Stockpile,
Mirrory serwisu www.freescosoft.com:
http://www.freescosoft.com/home/home.html - USA West Virginia,
http://www.freescosoft.org/home.html - Germany,
http://thelight.mine.nu/freescosoft/home.html - Netherlands,
http://freescosoft.abidjanville.com/home.html - France,
http://tecknojunky.dyndns.org/freescosoft/home.html - Canada,
http://dk.freescosoft.net/home.html - Denmark,
http://thetigger.dyndns.org/freescosoft/home.html - Sweden,
http://freescosoft.avaarsani.ca/home.html - Canada,
http://se.freescosoft.net/home.html - Sweden,
http://us-tx.freescosoft.net/home.html - USA Texas,
http://us-ct.freescosoft.net/home.html - USA Connecticut,
http://freescosoft.freebse.nl/home.html - Netherlands,
http://es.freescosoft.net/home.html - Spain

6. PAKIETY DLA FREESCO - KRÓTKI OPIS.

apache - bardzo dobry serwer www, zawiera moduł php,
apache_awstat - wizualizacja statystyk serwera apache na stronie www,
arp - zabezpiecza przed podpięciem się do naszej sieci,
bash - alternatywna powłoka systemowa (interpreter poleceń),
bind8 - serwer nazw w wersji 8 zastępuje standardowego binda 4,
bitchx - klient usługi IRC,ozwala na ircowanie z poziomu konsoli,
cron - pakiet, który pozwala uruchamiać dowolny proces o ściśle określonej godzinie,
dancer - boot IRC'owy, pozwala na utrzymanie na kanale IRC własnego nick'a,
eco-lib, lewy-lib - biblioteki potrzebne do działania niektórych pakietów,
exim - pocztowy serwer SMTP (Message Transfer Agent),

eXtremail - prosty w konfiguracji serwer pocztowy POP3 i SMTP,
fetchmail - pobiera pocztę z kont w sieci Internet i forwarduje ją na Fresco,
ftpd - serwer FTP, prosty w konfiguracji serwer FTP o ograniczonych możliwościach,
las - wyświetla statystyki serwera, wizualizuje ruch, jaki odbywał się na Freesco,
links - tekstowa przeglądarka stron www działająca z poziomu konsoli Freesco,
lynx - inna tekstowa przeglądarka stron www dostępna na Freesco,
mc - menadżer plików dla Freesco (przypomina wyglądem Norton Commandera),
msql - miniSQL - serwer bazy danych,
muh - utrzymuje twój nick na IRC'u,
mySQL - popularny serwer baz danych,
nmap - sprawdza, które porty naszego serwera są otwarte,
openssh - serwer ssh (secure shell) - szyfrowanego połączenia z Freesco,
perl - pakiet perl w wersji 5.0 - język skryptowy,
phpMyAdmin - administracja bazami danych mySQL, ze strony www,
portsentry - wykrywa skanowanie portów, pozwala odpowiedzieć tym samym :),
proftpd - bardzo dobry serwer FTP,
samba - serwer plików dla MS Windows,
squid - serwer proxy dla Freesco,
teapop - pocztowy serwer POP3, współpracuje z exim'em,
thttp - prosty serwer www, ze zintegrowaną obslugą php,
top - wyświetla informacje o pracy serwera (np. zajęcie procesora, itp.),
uptime - pokazuje czas działania Freesco od ostatniego restartu,
useradd - dodawanie użytkowników i grup na serwerze,
utils - dodatkowe narzędzia,
wget - do ściągania plików w tle, z serwerów http i ftp,
whois - identyfikuje komputery w Internecie,

7. Konfiguracja pakietów dla Freesco

7.1 Apache, php, mySQL, perl - serwer i usługi www
Chcąc mieć w pełni funkcjonalny serwer www musimy zainstalować pakiety: *apache*, opcjonalnie
apache-awstat - statystyki serwera, *mySQL i perl*. Jesli jeszcze nie zainstalowaliśmy, najpierw musimy zainstalowaa pakiet *lewy-lib* zawierający niezbedne biblioteki. Kolejny krok
to instalacja *apacha*. Wpisujemy *installpkg http://www.freesco.arx.pl/pakiety/apache* i wciskamy ENTER po pierwszym pytaniu, natomiast "y" i ENTER po drugim. Pojawi sie jeszcze ostrzeżenie, że *apache* potrzebuje pakietu *lewy-lib*. Także i tu odpowiadamy "y" na pytanie,
czy kontynuować i wciskamy ENTER. Ostatnie pytanie: "Czy chcemy zachowaa pliki w katalogu
www?", odpowiedź dowolna, należy pamietać jednak, że pliki poinstalacyjne zajmują nam miejsce na dysku, a im wiecej plików na dysku - tym dłużej startuje Freesco. Pozostaje
jeszcze reboot, przed rozpoczeciem używania serwera. W moim Freesco zmieniłem przed
uruchomieniem kilka linijek w pliku *httpd.conf*. W linii 290 ustawiłem *DocumentRoot "/mnt/home/www"* i tam przeniosłem strony. Wpis trzeba zmienia również w linii 315, 350, 532, 533,
539 (wszedzie tam należy uaktualnić scieżke dostępu). W linii 367 *DirectoryIndex index.html*
index.htm dopisałem jeszcze: i*ndex.php index.php3* oraz *index.cgi*. Zmieniłem również w linii 483 typ logu z *common* na *combined*. Oczywiście należy również dostosować wpis w linii 269
- adres e-mail admina. Warto również zmienic linie 331: *AllowOverride All*, taki wpis spowoduje,
że jeśli umieścimy w katalogu plik *.htaccess*, każdy odwiedzajacy bedzie pytany o hasło. Linia 449 - *HostnameLookups On* pozwala na wyświetlanie w logu nazw kanonicznych
(lub numerów IP przy opcji Off). Aby nie ułatwiać życia włamywaczom wyłczyłem również
opcję podawania sygnatury serwera, np przy błednych odwołaniach - *ServerSignature Off* w
linii 505. Taka konfiguracja pozwala na podstawowe działanie serwera, bez dodatkowych serwerów
wirtualnych - niestety tych opcji nie jestem w stanie przetestowac. Jeśli serwer apache
nie chce wystartować, należy oczywiście sprawdzić wszystkie pliki, upewnić sie, że mamy
potrzebne biblioteki i przejrzeć *error_log* w katalogu */mnt/router/packages/apache/logs*. W moim przypadku zaistaniała koniecznośa zmiany kernela na, doinstalowany wraz z *apache,*
kernel.586 - wówczas serwer zaczął poprawnie pracować. Wystąpiła taka sytuacja na Freesco
zainstalowanym bez plików startowych MsDOS.
Kolejnym potrzebnym elementem serwera jest *mySQL*. Instalacja jest prosta po wydaniu polecenia
installpkg ujrzymy, jak zwykle dwa pytania. Pierwsze: "czy chcemy przejrzeć skrypt?" (ENTER) i drugie: "czy kontynuować instalację?" ("y" i ENTER). I w tym momencie serwer
mySQL już działa - nie spotkałem się z żadnymi problemami podczas kilkukrotnej instalacji.
Odrebną sprawą jest jeszcze konfiguracja, należałoby utworzyć użytkownika baz *mySQL*
(domyślnie jest to *root*). Do administracji przydatny bedzie pakiet *phpMyAdmin*. Instalacja
jest standardowa, po jej zakonczeniu zobaczymy jeszcze ostrzeżenie przed udostepnianiem
publicznie tego narzedzia, autor pakietu radzi przenieść/zmienić katalog lub zastosować plik
.htaccess. To oczywiście jest truizm. Tak ważne narzedzie musi byc udostepnione tylko uprawnionej
osobie. Nie polecam zabezpieczania w pliku *config.inc.php* - tam hasło wpisane jest otwartym tekstem. Najlepiej użyć pliku *.htaccess*, który bedzie odwoływał się do pliku z
hasłami *.htpassword* w innym katalogu.

W pliku konfiguracyjnym możemy zmienić w linii 65 wpis *"english.inc.php"* na *"polish.inc.php"*
i phpMyAdmin bedzie się do nas odzywał po polsku.
Aby nasz serwer miał wszystkie opcje musimy jeszcze zainstalować pakiet *perl* i na koncu
apache-awstat. Instalacja *perla* nie sprawia żadnych kłopotów i nie zmusza nas do konfigurowania,
dlatego nie bede jej opisywał.
Pakiet *apache-awstat* służy do generowania statystyk serwera apache, korzysta z jego logów i posiada dość dużo opcji konfiguracyjnych. Po zainstalowaniu poddajemy edycji plik

awstats.conf i możemy zmienic tam wiele opcji, pierwszą z nich bedzie zmiana jezyka. W wierszu
94 musimy mieć: *Lang=6*. Wówczas statystyki bedą wyświetlane po polsku. Inne opcje konfiguracji należy przeawiczyć samemu, pamietając, aby skopiować sobie na wypadek błedu
oryginalny *awstats.conf*. W razie kłopotów zawsze możemy wrócić do oryginalnych ustawień.
To zastrzeżenie zresztą powinno być regułą przy edycji wszystkich plików konfiguracyjnych.
Zmiany należy wprowadzać pojedyńczo i testować przed zastosowaniem nastepnych.
Reasumując, instalacja nie jest trudna i w podstawowej konfiguracji powinna działać na
Freesco-box podłączonym do SDI, całość po zainstalowaniu na HDD zajmuje około 70MB.
Uwagi dodatkowe: Aby serwer spełniał swoje zadanie, szczególnie w zakresie obsługi *mySQL*,
musi być postawiony na komputerze przynajmniej Pentium i 32 MB RAM. Należy pamietać,
że jeśli na SDI udostepnimy *apache'a* dla zbyt wielu klientów, może to zatkać łącze, zatem
warto pogrzebać się w plikach konfiguracyjnych. Zwyczajowo też przypominam, że nie ponosze
żadnej odpowiedzialności za straty nerwów i inne spowodowane zastosowaniem się do moich rad.
Wymagane pakiety można znaleść na wielu stronach z pakietami. Polecam jednak instalować
z Polskiej Strony Freesco (*http://www.freesco.arx.pl*). Aby zainstalować pakiety nalezy wydać
komendy:
installpkg http://www.freesco.arx.pl/pakiety/lewy-lib
installpkg http://www.freesco.arx.pl/pakiety/apache
installpkg http://www.freesco.arx.pl/pakiety/phpMyAdmin
installpkg http://www.freesco.arx.pl/pakiety/perl
installpkg http://www.freesco.arx.pl/pakiety/apache-awstat
Autor: Maciek (maciek@pon.bytow.pl)

7.2 Obsługa poczty (exim, teapop, fetchmail, procmail, etc.)
Poczta elektroniczna, tzw. e-mail, jest realizowana przez programy nazywane MTA (Mail
Transport Agent). To te programy utrzymują skrzynki pocztowe użytkowników oraz zajmują
się skutecznym dostarczaniem listów do odbiorców. Programy wykorzystują standardowo port
25 komunikując się protokołem nazwanym SMTP (Simple Mail Transport Protocol). Niektóre z
tych programów potrafią także obsługiwać przekazywanie odebranych listów ze skrzynek do
programów obsługi poczty takich jak Outlook, The Bat itp. Tak jest w przypadku eXtremaila
ale np. Exim wymaga dodatkowego programu obsługującego protokół odbioru poczty nazywany
POP3. Odbiór poczty poprzez protokół POP3 odbywa się na porcie 110. Nowszy protokół
IMAP4 posługuje się portem 143.

Do dyspozycji we Freesco mamy kilka programów: eXtremail (SMTP + POP3) albo exim (SMTP)
we współpracy z teapopem (POP3) lub pakietem courier. Ponieważ eXtremail ma świetny opis
(manual) na swojej stronie domowej, a ponadto działanie tego programu było powodem wielu
problemów użytkowników Freesco, dlatego skupimy się na tandemie exim+teapop. Warto
polecić ostatnią wersję tych programów (exim 3.36, teapop 0.3.4) - o przyczynach takiego
wyboru później.
7.2.1 Instalacja
Poleceniem *installpkg http://adres.serwera.z.paczkami/exim* rozpoczynamy instalację exima
a później teapopa (zamiast teapopa można wybrać courier, który ma możliwość posługiwania
się protokołem IMAP4) Przykład: *installpkg http://www.freesco.arx.pl/pakiety/exim* Instalacja
jest standardowa i nie powinna sprawić większych kłopotów. Exim jest programem MTA, czyli
jedynie przekazuje pocztę pomiędzy komputerami w Internecie. Zatem nie sprawdzimy jego
działania przed instalacją programu do odbioru poczty.
7.2.2 Konfiguracja
Po instalacji musimy wyedytować plik "*configure*" w katalogu */mnt/router/packages/exim*. Nie ma sensu podawać tu pliku w całości ponieważ większość domyslnych ustawień zachowamy.
Natomiast te które są poniżej, musimy koniecznie zmienić. Niektórym zmiennym pliku *con-*
figure można przypisać kilka wartości - w tym przypadku oddzielamy je dwukropkiem. Spacje
można wstawiać ale nie ma obowiązku, są ignorowane.
primary_hostname = wpisz.adres.swojego.serwera.pl
# Przykład: primary_hostname = pp22.miastko.sdi.tpnet.pl
# qualify_domain =
# Zostawiamy zahaszowane, będzie wykorzystana wartość z primary_hostname
local_domains = localhost : wpisz.adres.swojego.serwera.pl
# Przykład: local_domains =
localhost:pp22.miastko.sdi.tpnet.pl:mojafirma.com.pl:jakisw
pis.domenakumpla.pl

Te linie wskazują Eximowi, po nawiązaniu połączenia przychodzącego w celu przesłania maila,
jakie przesyłki ma dostarczyć do lokalnych skrzynek a jakie należy przesłać dalej (tzw. relaying).
Jeśli adres docelowy e-maila nie zgadza się z którąś z wartości *local_domains* nie powinniśmy domyślnie pozwalać na przesyłkę dalej bez autentykacji, o czym później, ponieważ
stworzymy tzw. *open relay* chętnie wykorzystywany przez spamerów do nadużyć.
local_domains_include_host_literals
forbid_domain_literals
Pierwszą domyślnie haszujemy znakiem "#", drugą należy odhaszować, jeśli nie chcemy
dostawać maili zaadresowanych do nas za pomocą naszego adresu IP zamiast nazwy domeny.
Przykładowo user@[212.100.111.111] - jest to zaszłość używana dawniej choć nadal będąca

częścią standardu, jednak obniża odporność na otrzymywanie niepożądanej poczty.
never_users = root
Definiujemy użytkowników dla których lokalne dostarczanie listów nie będzie wykonywane
pod ich numerem *uid*, w zamian będzie użyte konto *nobody*. Jest to następna opcja bezpieczeństwa tzw. *paranoid*. Oczywiscie należałoby jeszcze zmienić wpisy w pliku "*aliases*"
(katalog */mnt/router/packages/mail*) - tak żeby listy adresowane do *roota* trafiały do innej skrzynki, posługiwanie się kontem roota do odbioru poczty nie jest bezpieczne.
Teraz pora na ustawienia dotyczące komputerów, które będą mogły korzystać z serwera *smtp*
(wysyłać listy w świat), domyślnie są to komputery w sieci wewnętrznej i ewentualnie zaufane
hosty naszych znajomych, czy nasz własny w pracy (lub odwrotnie). Ważne jest, żeby adresy
tych komputerów były stałe - nie będzie to działać ze zmiennymi IP przydzielanymi komputerom
łączącym się z internetem za pomocą modemów analogowych np. 0202122 w TPSA, usługa Dialnet co dzień itp.
host_accept_relay = localhost : my.friends.host : 192.168.0.0/16
Oczywiście nie wszystkie wpisy muszą być, jeśli jednak chcemy korzystać z logchecka, powiadamiania
sms na telefon komórkowy, czy polecenia "mail" w skryptach php czy cgi, musimy tu również umieścić wpis *localhost* i wewnętrzną nazwę naszego serwera (jeśli jest inna niż
nazwa zewnętrzna).
relay_domains =
To zostawiamy zachaszowane bo dotyczy tylko sytuacji gdy jesteśmy wpisani w DNS dla
jakiejś domeny zapasowym serwerem MX czyli poczty. Jeśli jednak jesteśmy to wpisujemy tu
te domeny dla których prowadzimy taką usługę.

7.2.3 Czynności końcowe.
Odblokujmy jeszcze komunikację programu ze światem. W tym celu wyedytujmy plik */mnt/*
router/rc/rcuser/rc_exim i wyszukajmy linijek:
Comment out the next line to make exim accessable from the internet
["$ENAMSQ" = y] && ipfwadm -I -a reject -P tcp -W $INET -D 0.0.0.0/0 25
Ta druga musi zaczynać się znakiem "#", jeśli go brak wstawmy go tam i zapiszmy zmiany
w pliku. Na tym można zakończyć konfigurację eximа dla najprostszej sytuacji, gdy listy
wysyłane w świat będą pochodzić tylko z komputerów w naszej sieci lokalnej. Jednak mogą
zaistnieć sytuacje, że sami znajdziemy się na zewnątrz sieci, albo udostępniamy komuś konto
e-mail. Temu służy tzw. autentykacja albo inaczej uwierzytelnianie.
host_auth_accept_relay = *
Gwiazdka wpisana w tej linii spowoduje, że ze wszystkich hostów zewnętrznych trzeba będzie
stosować uwierzytelnianie. Ostatnia sekcja pliku "*configure*" zawiera wpisy pozwalające korzystać z haseł systemowych w celu przeprowadzenia uwierzytelniania, w tym zakresie niczego
nie zmieniamy.

Pozostałe elementy konfiguracji można pozostwić bez zmian. Należy jednak wspomnieć o kilku
możliwościach. Obecnie popularnym formatem przechowywania poczty jest tzw. maildir. Exim
korzysta z tego domyślnie. W sekcji "*transport Configuration*" są następujące ustawienia:
local_delivery:
driver = appendfile
maildir_format = true
directory = /var/mail/$local_part
require_lockfile = true
use_fcntl_lock = true
use_lockfile = true
delivery_date_add
envelope_to_add
return_path_add
headers_add = "Lines: $body_linecount"
group = mail
# mode = 0660
Jeśli zmienimy "directory" na "file" exim będzie składował pocztę w tradycyjnym formacie
"mbox" czyli w pliku. Wielu administratorów Freesco pyta o możliwość założenia skrzynek
pocztowych w katalogach domowych, które zwykle są na osobnej partycji, zapobiega to zapchaniu
partycji systemowej przez użytkowników lubiących przesyłać i przechowywać wiele dużych plików. Musimy dokonać kilku zmian w konfiguracji eximа i teapopa. Przedstawiony
schemat zakłada, że katalogi użytkowników znajdują się w */mnt/home*.

Zmiany w pliku konfiguracyjnym eximа:
local_delivery:
driver = appendfile
# maildir_format = true
file = /mnt/home/$local_part/.Mailbox
require_lockfile = true
use_fcntl_lock = true
use_lockfile = true
delivery_date_add
envelope_to_add
return_path_add
headers_add = "Lines: $body_linecount"
group = mail
# mode = 0660
zmiany w pliku *teapop.passwd*:
empty:*:passwd:~/.Mailbox:0:
W ten sposób poczta będzie składowana w pliku .Mailbox w katalogu domowym użytkownika.
Wybrano tu tradycyjny format "*mbox*" ze względu na zapewnienie dobrej współpracy z linuxowym
klientem e-mail i news - *Pine*. Zastosowano nazwę pliku z kropką, co oznacza w linuxie plik ukryty i ma zapobiec przypadkowemu skasowaniu pliku podczas sesji ftp, oczywiście nie
będzie tragedii jeśli plik zniknie, exim założy go gdy następny raz przyjdzie poczta. Jeśli ktoś

wybierze taki format poczty, powienien również zmienić plik *aliases*, aby żadne komunikaty
nie przychodziły już na konto *root*.
Dlaczego warto przeprowadzić tę zmianę? Nie tylko ze względu na ulokowanie poczty. Zmiany
te pozwalają również na udostępnienie użytkownikom pliku *.forward* w katalogu domowym
(potrzebny np. do powiadamiania sms). Ponieważ właśnie jest przygotowywany pakiet *procmail*,
trzeba dodać, że dokonanie powyższych zmian jest warunkiem korzystania z procmaila.
Powyższy opis wykonany został na podstawie doświadczeń i prób, więc zawiera sprawdzone informacje. Olek i Maciek - autorzy opisu wykorzystali doświadczenia swoje i innych członków grupy trzepak.freesco, w ostatniej części opisu konsultacjami służył Mis'.
Autorzy: Olek (olotest@poczta.onet.pl),
Maciek (maciek@pon.bytow.pl),
*Mis' (*mis@hustons.homechoice.co.uk),

7.3 Proftp - serwer FTP
Proftpd jest uznawany za jeden z najlepszych serwerów ftp, zastosowanie go na serwerze
Freesco na pewno wpłynie na bezpieczeństwo, jak i sprawne przesyłanie plików. Instalacja
jest bardzo prosta, wystarczy wpisać polecenie:
installpkg adres_serwera_z_paczkami/proftpd
Następnie odpowiadamy "n" na pierwsze pytanie i "y" na drugie - i wszytko zostanie zainstalowane.
Ponieważ Freesco zostało pomyślane jako serwer dla niewielkich sieci domowych (szkolnych,
biurowych, osiedlowych), więc zaawansowane opcje serwerów wirtualnych nie są tu w zasadzie
potrzebne. Zatem sugeruję instalację ze strony Leszka Filipskiego (http://wydmy.republika.pl)
- ta wersja jest prosta i nie wymaga szczególnych umiejętności, zaś autor dołączył przykładowe
pliki konfiguracyjne i dokładny opis instalacji oraz konfiguracji.
Biorąc pod uwagę, że pracujemy na niezbyt pojemnych połączeniach zakładam, że serwer ftp
chcemy udostępnić w celu administrowania stronami www, trzeba się bowiem liczyć z tym, że
jeśli udostępnimy jakieś pliki światu, to kilku odwiedzających skutecznie może nam zapchać
dostęp do Internetu. Poniżej jest podstawowy plik konfiguracyjny podany przez Leszka Filipskiego
i nieco przeze mnie zmodyfikowany:

```
# Konfiguracja Proftpd
# Zawarto w nim konfigurację dla pojedynczego serwera i dla jednego
# login'u anonymous. W efekcie, aby miało to szansę zadziałać musisz
# mieć zdefiniowanego użytkownika/grupę "nobody"
ServerName "FTP serwer"
ServerType standalone
DefaultServer on
# Port 21 to standardowy port FTP.
Port 21
Umask 022
# Aby zabezpieczyć się przed atakami DoS (odmowa udostępnienia usługi)
# zaleca się ustawienie maksymalnej liczby procesów potomnych na 30
MaxInstances 30
# Ustaw użytkownika i grupę z poziomu których serwer normalnie startuje.
User nobody
Group nobody
# Normally, we want files to be overwriteable.
<Directory /*>
AllowOverwrite yes
</Directory>

# Podstawowa konfiguracja użytkownika anonimowego, bez upload'u katalogów.
<Anonymous /mnt/home/pub>
User nobody
Group nobody
# Potrzebujemy uzytkownika który będzie używany gdy ktos będzie się
# logował jako anonim. Tu po zalogowaniu się do serwera jako anonymous
# faktycznie będziemy korzystać z konta nobody
UserAlias anonymous nobody
# Maksymalnaliczbaużytkowników loguj&plusmn;cych się jako anonymous
MaxClients 5
# Tu ustawiamy fakt logowania bez hasła
AnonRequirePassword off
# 'welcome.msg' będzie wyświetlane w chwili logowania,
# a '.message' w każdym nowo otwartym katalogu.
DisplayLogin welcome.msg
DisplayFirstChdir .message
# Limit WRITE mówi czy można zapisywać cokolwiek w katalogu
# Dyrektywa DenyAll nie pozwala na to nikomu
# Inne możliwe dyrektywy to (nie wszystkie):
# AllowAll, Allow 192.168.1.*, AllowUser filip, DenyUser anonymous
# Oczywiście chodzi tu o środowisko 'chroot' stworzone dla
# użytkownika anonymous
<Limit WRITE>
AllowUser twoj_user
DenyAll
</Limit>
</Anonymous>
# koniec definicji użytkownika anonymous
DefaultRoot /mnt/home
# auth file - jesli chcesz możesz stworzyc dodatkowy plik, lub korzystać z systemowego,
bezpieczniej to pierwsze
AuthUserFile /mnt/router/etc/passwd
# początek definicji katalogu domowego użytkownika webadmin
<Directory /mnt/home/www>
AllowOverwrite yes
<Limit All>
AllowUser webadmin
DenyAll
</Limit>
</Directory>
# koniec definicji katalogu

# początek definicji katalogu
```

```
<Directory /mnt/home/twoj_user>
AllowOverwrite yes
<Limit All>
AllowUser twoj_user
DenyAll
</Limit>
</Directory>
# koniec definicji katalogu
# W zasadzie przydzielanie katalogów jak powyżej nie jest potrzebne,
# serwer domyślnie wpuszcza usera
# do jego katalogu domowego
# początek definicji serwera wirtualnego
<VirtualHost Twoja_domena.pl>
# Nazwa twojego hosta
ServerName "FTP Server"
TransferLog /mnt/router/packages/proftpd/var/virt_tran.log
# katalog root dla tego serwera (nie można wyjść ponad ten katalog)
DefaultRoot /mnt/home
# auth file
AuthUserFile /mnt/router/etc/passwd
# początek definicji katalogu domowego użytkownika webadmin
<Directory /mnt/home/www>
AllowOverwrite yes
<Limit All>
AllowUser webadmin
DenyAll
</Limit>
</Directory>
# koniec definicji katalogu
# początek definicji katalogu
<Directory /mnt/home/twoj_user>
AllowOverwrite yes
<Limit All>
AllowUser twoj_user
DenyAll
</Limit>
</Directory>
# koniec definicji katalogu

# początek szczegółowej definicji katalogu dla użytkownika anonumous
<Anonymous /mnt/home/pub>
User nobody
Group nobody
UserAlias anonymous nobody
MaxClients 10
<Directory upload>
# pobieranie plików dozwolone
<Limit STOR>
AllowAll
</Limit>
# nie wolno nic zapisywać
<Limit WRITE DIRS READ>
DenyAll
</Limit>
# można się poruszać po drzewie katalogowym
<Limit CWD XCWD CDUP>
AllowAll
</Limit>
</Directory>
</Anonymous>
</VirtualHost>
```

Część druga <VirtualHost> nie jest potrzebna przy podstawowej konfiguraci i można ją spokojnie wyciąć. Przyda się jeśli mamy wirtualne domeny. Ważne jest, że proftpd nie wpuści użytkownika powyżej katalogu DefaultRoot. Dlatego aby można było spokojnie administrować plikami i stronami www, a jednocześnie mieć pewność, że jakiś user nie podpatrzy nam pliku passwd, najlepiej umieścić wszystko w katalogu home. W katalogu /home umieszczamy pliki katalogi użytkowników i strony www (patrz konfiguracja apacza). I admin ma spokojną głowę.

Zaletą proftpd jest możliwość ustawienia dostępu tylko niektórym użytkownikom lub tylko adresom w sieci wewnętrznej. Jeśli nie chcemy aby kolega X wchodził na serwer będąc na wczasach, bo gapa na pewno zostawi swoje hasło w kafejce internetowej, ustalamy, że może logować się wyłącznie ze swojego komputera w domu.

W pakiecie znajdują się także dwa dodatkowe programy: *ftpcunt* - wyświetlający nam ilość zalogowanych userów i *ftpwho* - pokaże nam, kto jest zalogowany na naszym serwerze.

Tekst ten powstał na bazie opisu wykonanego przez Yachoo, a także inne uwagi uczestników grupy trzepak.freesco. Ponadto wykorzystałem informacje zawarte w artykule Dariusza Sobolewskiego w numerze 8/2000 czasopisma Linux+ i informacje autora instalowanego przeze mnie pakietu Leszka Filipskiego.

7.4 Squid - serwer proxy

```
# niom dopisać zostało #
# no i jeszcze squid działający przezroczyście dla przegladarki #
```

7.5 Samba - serwer plików

Zanim zainstalujemy sambę, należy sie zastanowić, czy naprawdę jej potrzebujemy? Jest to bowiem usługa wymagająca dość wydolnego komputera, jeśli ma działać poprawnie (pentium i 32MB RAM to minimum). Postaram się pokrótce wyliczyć sytuacje, w których samba może być potrzebna:

1. Sieć komputerowa w firmie (szkole...) w której istnieje potrzeba trzymania pod kontrolą komputerów z Windows, a raczej ich użytkowników. Samba może pracować jako kontroler domeny NT i uniemożliwić jakąkolwiek czynność bez zalogowania się do serwera. Także i wtedy jeśli potrzebny nam bezpieczny (w miarę) serwer plików, z którego np. będą uruchamiane

programy księgujące itp. Samba również sprawdza sie wg. wielu opinii jako serwer druku.
2. W sieci innego rodzaju (np. osiedlowej), w której jest silny serwer i wola użytkowników, aby
udostepniać wpólne zasoby, które mogą być "zrzucane" na serwer z komputerów domowych.
3. W sieci dowolnego typu, jeśli serwer ma pełnić rolę archiwum.
Instalacja samby, podobnie jak innych pakietów nie jest skomplikowana. Proponuję wybrać
pakiet samba ze strony Tigera, który przygotował też pakiet pomocny przy odinstalowaniu
wczesniejszych wersji (sambauninstfix) - pakiet jest dosyc spory (4,5MB), więc dobrze byłoby
poszukać, szybkiego serwera lub ściagnąć go i zainstalować lokalnie. Jak zwykle przy instalacji
musimy odpowiedzieć, czy chcemy przejrzeć plik instalacyjny (wciskamy "n") i czy kontynuować
instalację (wciskamy "y"). Ponieważ samba ma zapisane regułki blokujące dostęp z Internetu,
najlepiej wpisać reboot i ENTER. Jeśli będziemy używać samby w najprostszej konfiguracji,
możemy doinstalować pakiet sambaswat, który umożliwia kontrolę z poziomu przeglądarki
internetowej. Osobiście nie polecam tego rozwiązania, ze względu na bezpieczeństwo serwera,
jesli stanowi on jednocześnie bramkę do Internetu. Pakiet kontrolny swat komunikuje się na porcie 901 i wymaga uprawnień roota. Swat umożliwia nam kontrolę na poziomie
zabezpieczeń "share" i w tym przypadku jego stosowanie jest proste. Jeśli jednak zamierzamy
uczynić sambę kontrolerem domeny, jak każdy automat może nam strasznie "namieszać" w
pliku konfiguracyjnym. Po zrestartowaniu komputera samba zaczyna działać ze wszystkimi
domyślnymi ustawieniami. Możemy juz zobaczyc nasz serwer w otoczeniu sieciowym. pod
warunkiem, że w pliku */mnt/router/packages/samba/lib/smb.conf* ustawiliśmy wewnętrzne
adresy naszej sieci i ustalilismy jakie komputery mają z samby korzystać.
Adresy pakietów:
installpkg http://thetigger.dyndns.org/tiger/samba
installpkg http://thetigger.dyndns.org/tiger/samba.swat
installpkg http://thetigger.dyndns.org/tiger/sambauninstfix
Informacje na temat Samby:
http://www.samba.org - po angielsku
http://bofh.vt.pl/samba/ - po polsku

7.5.1 Samba - konfiguracja podstawowa
Linuxowy serwer samba ma wiele zalet, jedna z nich na pewno przerasta wszystkie inne. Jest
o kilka tysięcy złotych tańszy od Windows NT, czy Netware, kosztuje tylko kilkanaście minut
pracy przy komputerze - rozprowadzany jest bowiem na licencji GPL. Są poważne firmy, w
których samba wykorzystywana jest jako serwer plików i aplikacji oraz drukarek. Jeśli jednak
marzysz o tym, aby po kliknięciu myszką twojemu userowi wyskakiwał napis: "Kliknięcie jest
niemożliwe z powodu ograniczeń nałożonych na ten komputer", a cała administracja również
ograniczała się do klikania, to jesteś potencjalnym klientem Micro$oftu. Samba na pewno nie
będzie też konkurować z Novellem. Zainstalujemy więc sambę, jeśli mamy małą sieć i potrzebujemy
wydajnego i stabilnego serwera, który poradzi sobie ze wszystkimi zadaniami.
Po instalacji musimy przystąpić do konfiguracji. Samba ma jeden plik konfiguracyjny - *smb.conf*. Najpierw konfiguracja w wersji podstawowej. Musimy ustawić w sekcji *[global]* kodowanie polskich liter dla windozy i linuxa, podać interfejs naszej sieci i komputery, którym
pozwolimy korzystać z zasobów serwera. Kolejnym krokiem będzie ustawienie ścieżek do
udostępnionych katalogów. Jeśli korzystamy z Windows 98, powinniśmy dodać jeden wpis w
rejestrze:
[HKEY_LOCAL_MACHINESystemCurrentControlSetServicesVxDVNETSUP]
"EnablePlainTextPassword"=dword:00000001
Związane jest to z różnym kodowaniem haseł w Windows i Linuxie, każemy zatem windozie
aby nie kodowała haseł. Windows 95 nie potrzebuje tego wpisu, zaś jeśli komputery klienckie
pracują pod kontrolą nowszych wersji Windows, musisz odwiedzić witrynę:
www.samba.org
Znajdziesz tam wskazówki jak przystosować swój Windows do pracy z sambą.
Pod adresem: *ftp://pl.samba.org/pub/unix/net/samba/docs/Registry/* - można znaleźć potrzebne wpisy do rejestru, jako odpowiednie pliki *.reg do różnych wersji Windows.
Poniżej podaję zawartość podstawowego pliku konfiguracyjnego:

```
##----------------------------------- plik smb.conf -------------------------------------
-
# Plik konfiguracyjny smb.conf w wersji podstawowej
# Samba jako serwer plikow - bez funkcji kontrolera domeny

# Parametry glowne
# Ustawiamy kodowanie (linie -1,2), interfejs sieci (4), poziom zabezpieczen (5),
# z potrzebnych w tej sekcji ustawień - jeszcze host allow (22), w tym przypadku
# jest to localhost i wszystkie komputery z sieci. Pozostale parametry sa domyslnie
# ustawione, lecz nie maja wiekszego znaczenia
[global]
client code page = 852
character set = ISO8859-2
server string = Samba Freesco Server
interfaces = 192.168.1.1/24
security = share
domain logons = yes
domain master = yes
local master = yes
preferred master = yes
logon script = %u.bat
logon path = \nazwa_serwera\mnt\home\netlogon
encrypt passwords = No
smb passwd file = /mnt/router/etc/passwd
log file = /mnt/router/packages/samba/var/samba.%m
```

```
max log size = 5
read raw = No
read size = 8192
socket options = TCP_NODELAY IPTOS_LOWDELAY
wins proxy = Yes
wins support = Yes
guest ok = Yes
hosts allow = 127. 192.168.
# sekcja katalogu domowego, kazdy user widzi swoj katalog domowy, pod
warunkiem,
# ze user na windozie loguja sie takim samym loginem jak w linuxie (potrzebne
haslo)
[homes]
writeable = yes
browseable = no
create mode = 660
directory mode = 770

# katalog logowania - w wersji share, w zasadzie niepotrzebny
[netlogon]
comment = domain logon service
path = /mnt/home/netlogon
preexec = csh -c '/mnt/router/usr/bin/netlogon %u' &
guest ok = No
# katalog dostepny dla wszystkich
[public]
comment = Katalog publiczny
path = /mnt/home/samba/public
read only = Yes
# katalog do ktorego bedzie potrzebne haslo - usera z grupy users
# (haslo uniksowe z /etc/passwd)
[sekretariat]
comment = Dokumenty
path = /mnt/home/samba/sekretariat
public = no
writable = yes
printable = no
valid users = @users
force group = users
force user = root
create mode = 660
directory mode = 770
##---------------------------- koniec pliku smb.conf ----------------------------------
-
```

Taka konfiguracja będzie nam działać pod warunkiem, że mamy ustawione prawidłowo
katalogi oraz użytkowników i grupy, którym pozwalamy korzystać z zasobów. Opcja *valid*
user pozwala ustawić uzytkownika do dowolnego zasobu, chcąc z niego skorzystać musimy
podac hasło, które ma ów user w pliku */etc/passwd* - stąd wniosek, że zasoby muszą być udostępnione użytkownikom systemowym.

7.5.2 Samba jako kontroler domeny

Samba może pełnić funkcję kontrolera domeny NT. Oznacza to, że zamiast Windows NT server,
możemy postawic komputer z Linuxem, co to oznacza dla małej firmy, czy sieci szkolnej
- nie trzeba tłumaczyć. Żeby ustawić sambę w tej roli, trzeba zastosować znacznie bardziej
złożony plik konfiguracyjny. Musimy też wszystkich użytkowników linuxowych dodać jako
użytkowników samby.
We Freesco wygląda to następująco: mamy użytkownika *user1* zapisanego w pliku */etc/passwd*, wywołujemy teraz: *smbpasswd -a user1* pojawi się monit o wpisanie hasła i powtórzenie
go jeszcze raz. Użytkownik został dodany i od tego momentu może korzystać z przydzielonych mu zasobów. Szczegółowy i bardzo dobry opis instalacji, konfiguracji oraz
objaśnienia znalazłem w artykule Bartka Siębaba na stronie *http://bofh.vt.pl/samba/* - jest to
tekst prosty i pozwalający zrozumieć zasady działania aplikacji, również plik konfiguracyjny
działa bez zadnych problemów.
Ze względów bezpieczeństwa zdecydowałem się na użytkowników samby, którzy nie będą
mieli dostępu do serwera. Tu trzeba dokonać pewnej ręcznej korekty. Z pliku */mnt/router/etc*
usunąłem hasła zastępując je znakiem *x* lub *!* i jako katalog domowy wpisałem */dev/null* a
powłoke */bin/false*. W ten sposób użytkownik mający pełnie uprawnień w Windows, nie będzie
groźny dla systemu - jest to dmuchanie na zimne, na wypadek gdyby nastąpiło włamanie
przez maskaradę do komputerów z Systemem Windows. Rzecz jasna samba jest niedostępna
z zewnątrz, co zapewniają odpowiednie wpisy w *rc_smbd*. System przeskanowany programem
Nessus nie wykazał niebezpieczeństwa w tym zakresie.
Po dodaniu użytkowników, musimy skonfigurować *smb.conf*, ze względu na oszczędność miejsca usunąłem komentarze:

```
## ---------------------------------------- plik smb.conf ------------------------------
-------
[global]
comment = Serwer Helios
log file = /mnt/router/packages/samba/var/%I.log
dont descend = /dev,/proc,/etc,/bin,/mnt,/sbin,/usr
socket options = TCP_NODELAY SO_SNDBUF=16384 SO_RCVBUF=16384
IPTOS_LOWDELAY
write raw = yes
getwd cache = yes
write cache size = 65536
netbios name = helios
debug level = 2

debug timestamp = no
timestamp logs = True
max log size = 300
bind interfaces only = True
```

```
interfaces = 192.168.1.1/255.255.255.0
hosts allow = localhost, 192.168.1.0/255.255.255.0
# printing = bsd
# printcap name = /etc/printcap
# map archive = no
# status = yes
# public = no
# read only = no
# lpq cache time = 10
preserve case = yes
short preserve case = yes
strip dot = no
hide dot files = yes
client code page = 852
character set = iso8859-2
security = server
guest ok = no
browseable = yes
create mode = 0700
# admin users = root
unix realname = yes
dos file times = yes
workgroup = workgroup
dead time = 15
keep alive = 15
mangled stack = 100
shared mem size = 1048576
max open files = 500
domain master = yes
local master = yes
preferred master = yes
wins support = yes
os level = 64
nt smb support = yes
nt pipe support = yes
nt acl support = no
domain logons = yes
logon script = %U.bat
logon path = \%Lprofiles%U
logon home = \%Lprofiles%U

# time server = True
name resolve order = wins bcast hosts lmhosts
unix password sync = false
update encrypted = no
passwd program = /bin/passwd %u
passwd chat debug = false
passwd chat = *New*password* %nn *Retype*new*password* %nn
*updating*done*
encrypt passwords = yes
null passwords = false
server string = Serwer Helios
[homes]
# kazdy user zobaczy swoj katalog (pod warunkiem ze jest userem systemowym)
comment = Twój katalog
# prawa do plików i katalogów tylko dla właściciela
create mode = 0700
directory mode = 0700
public = no
writable = yes
path = /mnt/home/%U
browseable = no
# "oplock" = "opportunistic lock"
oplocks = True
level2 oplocks = True
# veto oplock files = /*.DBF/*.dbf/
[netlogon]
comment = katalog logowania
path = /mnt/home/netlogon
case sensitive = no
create mode = 0755
directory mode = 0770
guest ok = yes
locking = no
writable = no
share modes = no
browseable = nowrite list = @root
[profiles]
path = /mnt/home/profiles
case sensitive = no
create mode = 0777
directory mode = 0777
guest ok = yes
locking = no
writable = yes
share modes = no

browseable = no
write list =@root
# [drukarka]
# path = /home/tmp
# comment = HP Desk Jet 600
# writable = yes
# printable = yes
# create mode = 0700
# read only = yes
# write list = @pub
# hosts allow = 10.0.0.1 10.0.0.100 10.0.0.110
# tą komendą Samba będzie drukować
# print command = /usr/bin/lpr -r -h -P %p %s
[public]
path = /mnt/home/samba/public
volume = public
comment = Katalog publiczny
browseable = yes
create mode = 0770
directory mode = 0770write list = @biuro
oplocks = True
level2 oplocks = True
hosts allow = 192.168.1.0/255.255.255.0
```

```
[biuro]
path = /mnt/home/samba/biuro
volume = biuro
comment = Katalog sekretariatu
browseable = no
create mode = 0770
directory mode = 0770
write list = @biuro
oplocks = False
dos filetime resolution = True
#[www]
#path = /mnt/home/www
#volume = www
#comment = Dla stron WWW
#create mode = 0770
#directory mode = 0770
#write list = @root
#oplocks = false
#level2 oplocks = false
## ---------------------- koniec pliku smb.conf ----------------------------------------
-
```

Ten plik konfiguruje sambę na serwerze sieci szkolnej obsługującej nie tylko pracownię, ale
także biuro - zatem jest katalog dostępny dla wszystkich do odczytu np. w celu umieszczania
ogólnie dostepnych upgrade'ow itp. Katalog biuro jest katalogiem do którego ma dostęp sekretarka,
dyrektor... Mogą z niego byc uruchamiane takie programy jak np. płace i kadry (DOS) - aplikacje nie robi wpisów w rejestrze.
Oczywiście w zależności od potrzeb należy konfigurację dostosować. No i na koniec mała łyzka
dziegciu. Jeśli ktoś zamierza zastosować sambę w tej konfiguracji i z takim zastosowaniem to
komputer musi być dość mocny - moje P166 i 32MB RAM to absolutne minimum.
Autor: Maciek (maciek@pon.bytow.pl)

7.6 Inne usługi (ssh, telnetd, etc)
7.6.1 whois - identyfikacja komputerów w Internecie.
Wśród narzędzi administratora jest wiele pożytecznych drobiazgów i do nich na pewno należy
pakiet, który do Freesco przygotował Mis'. Instalacja jest banalnie prosta i standardowa,
natychmiast po zainstalowaniu możemy używać polecenia *whois* w celu identyfikowania komputerów
w Internecie. Jest to pożyteczne narzędzie umożliwiające nam np. sprawdzenie skąd nastapiła próba włamania. Polecenie *whois* dostępne jest nie tylko z konsoli roota, ale także
zwykłego użytkownika, który ma dostęp do shella.
Składnia polecenia:
whois NR_IP - wyświetli nam wszelkie informacje znajdujące się w bazie ripe.net,
whois -n nazwa_serwera - pokaże nam mumer IP serwera,
whois -u nazwa_serwera - numer IP oraz wiele dodatkowych informacji,
whois -a nazwa_serwera - adresy e-mail na które można pisać ewentualne skargi na zachowania użytkowników z danej klasy adresów.

Szczegóły w pliku README w katalogu */mnt/router/packages/whois* - naprawdę warto ten pakiet zainstalować, zwłaszcza, że zajmuje niewiele ponad 20kB. W związku z tym, że czasami
brak informacji o polskich serwerach, kilka słów objaśnienia od autora pakietu:
"ten klient działa w ten sposób, że sprawdza w jakiej bazie ma szukać konkretnej domeny/ adresu IP i zwraca sie do lokalnego serwera... podczas testów wyszło mi, że to NASK ma niekompletne bazy... ponieważ mało wiem o procedurze rejestracji lub uaktualniania wpisów w bazie, więc nie chcę nic złego mówić o NASK-u. Poza tym jeśli RIPE zwraca przekierowanie na inny serwer to ten klient podąża za takim przekierowaniem...
Ten pakiet może być również przydatny dla zwykłego usera... potrafi wyszukać adresy pod które można wysyłać reklamacje, poskarżyć się na spam z danego serwera itp... chwilowo niestety działa z linii komend, więc user musi być zalogowany na serwerze (telnet, ssh). Planuję przygotować paczkę z whois działającym z interfacem (międzymordziem) www, ale to za jakiś czas..."
Dla leniwych - uproszczona wersja *whois* została napisana w php i działa z poziomu przeglądarki,
podaje jednak tylko podstawowe namiary numeru IP, działa skutecznie w przypadku SDI, ale
inne adresy moga nie zawierać żadnych potrzebnych nam informacji.
Autor: Maciek (maciek@pon.bytow.pl)

7.6.2 procmail - zawansowane filtrowanie poczty.
Procmail jest aplikacją, która służy do zaawansowanego filtrowania poczty. Umożliwia użytkownikowi usuwanie automatyczne niechcianych listów, przekierowanie poczty na inne
konta, wysyłanie kopii listu na inne konto mailowe, czy zapisywanie kopii w wybranym folderze.
Instalacja jest nieskomplikowana.
Procmail musi być wywoływany, po nadejściu przesyłki, przez exima, więc trzeba zrekonfigurować
ten program. Po pierwsze należy w */mnt/router/etc* umieścić plik "*users_aliases*" (i skopiować go
do */etc*) - może być on pusty, ale jego podstawowa zawartość powinna wyglądać tak:
user: user@twoj.serwer
user1: user1@twoj.serwer
Można w tym pliku zdefiniować userów nie istniejących w systemie, czyli dać możliwość używania
aliasów pocztowych, np.:
biuro: user1@twoj.serwer
Następnie trzeba umieścić pliki "*.procmailrc*" i "*.forward*" w katalogu domowym użytkownika.
Muszą one mieć *chmod 644* i być własnością użytkownika. Pierwszy z nich będzie zawierał
reguły rządzące pocztą i o nim później. Drugi zawiera ścieżkę do procmaila i ma następującą
zawartość:
"|/mnt/router/packages/procmail/bin/procmail"
(UWAGA! razem z cudzysłowami)
Ten plik nie jest we freesco niezbędny, procmail może działać bez niego (w czasie testów procmail
działał na komputerze z plikiem *.forward* zawierającym powiadamianie sms), jednak w razie kłopotów procmailem należy ten plik umieścić. Obydwa pliki muszą być własnością danego
użytkownika i grupy *mail*.
Kolejna sprawa to zmiana konfiguracji poczty. Jeśli poczta składowana jest w katalogach

domowych, należy w katalogu użytkownika bezwzględnie umieścić plik .procmailrc (nawet jeśli
użytkownik nie zamierza filtrować poczty) o następującej treści (kilka przykładów w zależności
od formatu i umiejscowienia poczty):

```
PATH=/bin
MAILDIR=/var/spool/mail/nazwa_usera/ # (/) obowiazkowo slash na końcu!
DEFAULT=$MAILDIR
LOGFILE=$MAILDIR/procmail.log #opcja
```

W powyższym przykładzie poczta składowana jest w domyślnym formacie exima dla freesco,
czyli maildir - katalogi.

```
SHELL=/bin/sh
PATH=/bin:/usr/bin:/mnt/router/packages/procmail/bin
MAILDIR=/var/spool/mail/nazwa_usera #ścieżka do katalogu poczty
DEFAULT=$MAILDIR #nazwa skrzynki pocztowej
LOGFILE=$MAILDIR/procmail.log #opcja
```

Powyżej przykład składowania poczty w formacie mbox - czyli pliki, w domyślnym katalogu instalowanym
przez exima.

```
SHELL=/bin/sh
PATH=/bin:/usr/bin:/mnt/router/packages/procmail/bin
MAILDIR=$HOME #ścieżka do katalogu poczty
DEFAULT=$MAILDIR/.Mailbox #nazwa skrzynki pocztowej
LOGFILE=$MAILDIR/procmail.log #opcja
```

W tym przypadku skrzynka pocztowa w formacie mbox w katalogu użytkownika.
Katalog przechowywania poczty może być dowolny pod warunkiem, że nazwa pliku z pocztą
(w formacie mbox) będzie nazwą użytkownika, w przeciwnym wypadku dostarczanie poczty
przestaje działać. Można umieścić pocztę na tej samej partycji, co katalogi użytkowników, ważne
jest tylko wykonanie dowiązania symbolicznego do /var/spool/mail, jeśli nie jest ona w katalogach
domowych. Jeśli nie zmieniamy miejsca położenia poczty, linkowana jest ona przez plik
rc_spool. W przypadku zmiany katalogu z pocztą należy zmienić odpowiednie wpisy w tym pliku
lub go usunąć i ręcznie wykonać dowiązanie symboliczne w pliku *rc_exim*, np. *ln -s /mnt/home/
poczta /var/spool/mail*. Uwagi te są istotne dla administratorów mających na serwerze więcej
niż jedną partycję.

Konfiguracja exima do stosowania procmaila:

W sekcji *TRANSPORT CONFIGURATION* po części *local_delivery* dodajemy:

```
# Procmail transport
procmail:
driver = pipe
command = "/mnt/router/packages/procmail/bin/procmail -Y -d ${local_part}"
```

W razie problemów usunąć nawias klamrowy w ostatnim fragmencie. Pamiętać trzeba o tym,
żeby w części *local_delivery* była podana prawidłowa ścieżka do plików lub katalogów z pocztą.

W sekcji *DIRECTORS CONFIGURATION* po *system_aliases*:

```
users_aliases:
driver = aliasfile
file = /etc/users_aliases
search_type = lsearch
errors_to = root
```

oraz po *userforward* jeszcze wpisujemy linie dotyczące procmaila:

```
# Procmail director
procmail:
driver = localuser
transport = procmail
require_files = /mnt/router/packages/procmail/bin/procmail
```

Konfiguracja teapopa wymaga sprawdzenia naszego wpisu na końcu pliku teapop.passwd. Powinien
on w tym przypadku wyglądać następująco (wersje w zależności od formatu i umiejscowienia
poczty):

```
empty:*:passwd:~/.Mailbox:0: # poczta w katalogu domowym (mbox)
empty:*:passwd:/var/spool/mail:0::mail: #poczta w katalogu domyślnym (mbox)
empty:*:passwd:/var/mail/:: # ustawienia standardowe (maildir)
```

Kolejnym krokiem jest umieszczenie w katalogu użytkownika pliku *.procmailrc* z regułami filtrowania
poczty. Jak ten plik ma wyglądać, można zobaczyć odwiedzając kilka adresów internetowych:

```
http://bobo.fuw.edu.pl/~lukow/hoohoo/procmail.pl.html
http://terror.black.art.pl/~look/linux/procmail-tips.html
http://ptm.linux.pl/man_HTML/man1/procmail.1.html
http://ptm.linux.pl/man_HTML/man1/formail.1.html
http://ptm.linux.pl/man_HTML/man5/procmailex.5.html
http://ptm.linux.pl/man_HTML/man5/procmailrc.5.html
```

Listy z dowcipami przesyłamy do dwóch kolegów, a ze swojego konta je kasujemy. (Uwaga! na
początku reguły jest zero):

```
:0
* ^To:.*user@moj.serwer
* ^Subject:.*dowcipy
{
:0 Ac
! kolega@jego.domena.pl
:0 Ac
! drugi.kolega@inna.domena
:0 A
/dev/null
}
```

Listy od kolegi przesyłamy na inne konto i zapisujemy w katalogu "dowcipy-news", co oznacza,
że listy z tematem dowcipy od kogoś innego niż "kolega" nie będą podlegały tej regule.

```
:0 c
* ^From.*kolega
* ^Subject:.*dowcipy
! user@jakis.serwer
:0 A
dowcipy-news
```

W tym przykładzie może być konieczne podanie ścieżki bezwzględnej do katalogu (pliku).

```
:0 c
```

** ^Subject:.*DOOM*
! nazwa_innego_usera@localhost
Reguła, która wysyła kopię na skrzynkę nazwa_innego_usera (każdy sobie musi wpisać jakiś
istniejący adres) jeśli w temacie listu znajdzie się ciąg znaków "DOOM".

Uwaga! Regułki (jeśli jest ich niewiele) można wpisać bezpośrednio w pliku *.procmailrc*, ale sensowniejsze
wydaje się wywoływanie regułek posegregowanych tematycznie(?) Wg. Zawartości z osobnych plików. Robi się to dodając w pliku *.procmailrc* linie:
INCLUDERC=/ścieżka/do/pliku/plik_z_regułami filtrującymi
Można podać wiele takich linii do różnych plików z regułkami. Bardzo ważna uwaga! Podczas
pracy procmaila każdy e-mail przetwarzany jest osobno. Reguły Filtrowania sprawdzane są kolejno
aż któraś zadziała, następne nie są już testowane... Wynika z Tego że kolejność zapisu reguł
jest bardzo istotna... Jeśli z jakichś powodów chcemy aby pomimo "pasowania" jakiejś reguły
inne też były sprawdzane należy do wywołania reguły dodać opcję "c" (bez cudzysłowu) np:
:0 c
Więcej na temat reguł filtrowania poczty można przeczytać w manach. Przykłady wstawiania
reguł filtrujących z osobnych plików:
INCLUDERC=$HOME/regula1.rc
jeśli poczta jest w pliku *.Mailbox* w katalogu domowym lub:
INCLUDERC=/mnt/home/user/regula1.rc
wtedy, gdy zostawiliśmy domyślne katalogi i format przyjmowany przez exima.
Brak n arazie danych o pracy procmaila z pakietem courier POP3 i IMAP. Gdyby komuś się
udało zmusić procmaila do pracy z courierem prosimy o informację i opis konfiguracji. Najlepiej
mailem na: *mis@hustons.homechoice.co.uk*, *olotest@poczta.onet.pl*, *freesco@pg241.slupsk.sdi.topnet.pl*. Biorąc pod uwagę możliwości protokołu imap zarządzania pocztą na serwerze i siłę
procmaila do sortowania poczty może to być świetne narzędzie.
Pakiet przygotował Mis', przetestowali z pomocą autora - Maciek i Olek, a efektem tego jest nasz opis. Procmail w połączeniu z eximem działa pod freesco, autorzy pakietu wykorzystali potencjał Procmaila tworząc mini listę dyskusyjną za pomocą której wymieniali uwagi i pomysły odnośnie konfiguracji procmaila pod freesco.
Autorzy: Maciek (emti@and.pl),
Olek (olotest@poczta.onet.pl),
*Mis' (*mis@hustons.homechoice.co.uk),

7.6.3 fnews - kożystanie z news za pomocą klienta poczty e-mail.
Fnews jest aplikacją pozwalającą na używanie klienta e-mail (np. The Bat) jako czytnika grup
dyskusyjnych, inaczej mówiąc jest to bramka e-mail - news. Pakiet dla Freesco przygotował Mis'.
Instalacja pakietu jest standardowa i nie wymaga wyjaśnień.
Konfiguracja i użytkowanie
Po instalacji program jest natychmiast dostępny, jednak żeby go użyć musimy utworzyć i dokonać
konfiguracji pliku */etc/fnewsrc* lub *~/.fnewsrc* (katalog domowy usera). Jeśli użytkownicy mają
dostęp do shella i chcą oraz potrafią samodzielnie zastosować "fnews", wówczas plik konfiguracyjny
pod nazwą *.fnewsrc* (plik ukryty) umieszczamy w katalogu domowym. W katalogach domowych umieszczamy ten plik również w sytuacji gdy użytkownicy subskrybują różne grupy.
Najpierw jednak utworzymy na serwerze konto "*news*" z hasłem "*hasło*" (uwaga, to tylko
przykład) służące do wysyłania postów. Ten użytkownik musi mieć swój katalog domowy, ale nie
musi mieć przypisanej powłoki, ponieważ nie będzie się logował (może być */bin/false*).
Następnie potrzebne dane, w tym serwer news, serwer smtp i pop3 (lokalne), umieszczamy w
pliku konfiguracyjnym. Ważną opcją przed pierwszym użyciem jest ustawienie *fetchlimit = 20*
(lub 50), ponieważ fnews zaczyna ściąganie postów od najstarszych. Gdybyśmy pozwolili na
ściągnięcie wszystkiego, najprawdopodobniej skończyłoby się to zatkaniem serwera i/lub konta
użytkownika. Poniżej przykładowy plik konfiguracyjny:
 # ports for all servers are optional
nntp = news.trzepak.pik-net.pl # name of nntp serverand port,
 # overriden by $NNTPSERVER
smtp = twoj.serwer.pl # name of smtp server and port
pop3 = twoj.serwer.pl # name of pop3 server and port
 # pop3 = stdin # fetchmail->some filter->pnews->nntp server
pop3user = news # account at the pop3 server
pop3pass=hasło # password for the pop3 server account
 # if it has spaces put " around it
mail=news@twoj.serwer.pl # name of sender
rcpt = user@twoj.serwer.pl # names of recipients
#localhost=mail.localnet.com # name of localhost
verbose = 1 # verbosity
 # 0 - error messages only
 # 1 - error messages and short progress explanation
 # groups to fetch or post, overriden by command line option '-f'
 # it may be a semicolon separated list of groups, see 'rcpt'
grouplist = ~/.fnewsgroups

 # Local MDA or any program that reads from standard input
 # Fetched messages will be piped to the command stdin
mda = "mail user@twoj.serwer.pl"
fetchlimit = -1 # Fetch all available articles
 # fetchlimit = 100
 # Fetch max 100 messages per session
 # groups to fetch or post, overriden by command line option '-f'
 # it may be a semicolon separated list of groups, see 'rcpt'
grouplist = ~/.fnewsgroups
Kolejnym krokiem jest utworzenie w katalogu domowym pliku .fnewsgroups i wpisanie w nim
interesujących nas grup. Jeżeli nie wiem jakie są grupy, z linii poleceń wpisujemy fnews -g i
otrzymamy listę grup np.:
**freesco*helios~/>fnews -g*
Connecting to news.trzepak.pik-net.pl at port 119: .. done.

trzepak 0000004572 0000002240 y
trzepak.networking 0000020687 0000008196 y
trzepak.his 0000010457 0000004883 y
trzepak.freesco 0000017895 0000003143 y
W pliku tym zapisujemy jedynie nazwę grupy (grup) która nas interesuje np. *trzepak.freesco*.
Uwaga! Jeśli zastosujemy te metodę dla *news.tpi.pl,* będziemy oglądać wyświetlanie nazw grup
przez conajmniej godzinę. Ostatnim elementem jest utworzenie katalogu */.news* - w którym
pojawią się pliki o nazwach ściąganych przez nas grup. Pliki *.fnewsrc* i *fnewsgroups* muszą mieć
chmod 600, katalog standardowo *755*.
Pora zatem na pierwsze wywołanie programu:
**freesco*helios~/>fnews*
Connecting to news.trzepak.pik-net.pl at port 119: .. done.
Fetching in trzepak.freesco (17895 to 17895)
Article 3298 (+14595): ..... done.
Article 3299 (+14594): ..... done.
/ciach/
Article 3302 (+14591): ..... done.
Article 3303 (+14590): ..... done.
Disconnecting from news.trzepak.pik-net.pl: done.

Ponieważ już wcześniej sprawdziliśmy ilość postów w interesującej nas grupie teraz jeszcze pozostaje
zmienić zawartość pliku *trzepak.freesco* w katalogu */.news* - zmieniamy tam liczbę na tę która jest mniejsza od ogólnej ilości postów o powiedzmy 50 (czyli 17895 a wpisujemy 17850).
Teraz w konfigu zmieniamy *fetchlimit = -1*, żeby odtąd ściągane były wszystkie nowe dostępne
posty.
Jeśli plik konfiguracyjny jest w katalogu stworzonego przed chwilą usera, możemy sobie używac
tego konta tylko do czytania newsów. Jednak to konto naprawdę potrzebne nam jest tylko do
wysyłania listów na grupę - więc wszystkie powyższe czynności wykonujemy w katalogu realnego
usera, który chce czytać newsy.
Teraz zamierzamy odpowiedzieć lub wysłać post na grupę dyskusyjną. Ze swojego normalnego
konta na które otrzymaliśmy newsy piszemy zwyczajny e-mail adresując go:
user@twoj.serwer.pl (trzepak.freesco)
List wędruje więc na to konto i wówczas wywołujemy z lini pleceń:
**freesco*helios~/>pnews*
Connecting to twoj.serwer.pl at port 110: .. done.
Connecting to news.trzepak.pik-net.pl at port 119: .. done.
List został wysłany.
Żeby zautomatyzować te czynności, trzeba uruchomić program z crona (mając plik */etc/*
fnewsrc)
**/15 * * * * fnews*
**/20 * * * * pnews*
Inny sposób to założenie z pozycji roota pliku o nazwie usera w katalogu */var/spool/cron*, który
korzysta z newsów (właścicielem pliku jest *root*, *chmod 600*) o treści:

**/10 * * * * /mnt/router/packages/fnews/fnews $* > /mnt/home/user/fnews.log*
Ten drugi sposób spowoduje automatyczne pobieranie newsów co 10 minut.

Można zautomatyzować pobieranie i wysyłanie postów przy zastosowaniu procmaila (jeśli plik
konfiguracyjny znajduje się w katalogu domowym). Reguła poniżej najpierw kieruje przesyłkę
do pliku .Mailbox (format mbox), a następnie uruchamia pnews - czyli wysyłanie listów do grupy.
Ostatnim krokiem jest pobranie nowych przesyłek, w tym własnego ostatniego listu.
:0
** ^To.*trzepak.test*
{
:0 c
.Mailbox
:0 fhbw
** ^To.*trzepak.test*
|/mnt/router/packages/fnews/pnews $ > pnews.log*
:0 fw
|/mnt/router/packages/fnews/fnews $ >fnews.log*
}
Taki filtr wpisany w plik *.procmailrc* ma jedną wadę, otóż zakłada aktywnego użytkownika,
który zawsze odpisuje na newsy (lub często pisze). Ponieważ pobranie newsów dokonuje się po
wysłaniu listu. Można temu zaradzić dopisując drugą regułę:
:0
** ^Subject:.*get-news*
{
:0 fw
|/mnt/router/packages/fnews/fnews $ >fnews.log*
:0
/dev/null
}
W ten sposób wysłanie na ten sam (przeznaczony do newsów) adres pustego listu z tematem
"get-news" spowoduje pobranie newsów z serwera, list następnie jest kasowany.
Autor: Maciek (emti@and.pl)

8. OGRANICZENIA FREESCO

8.1 Czy mogę skompilować programy/używać CDROMU/zainstalować Freesco na dysku SCSI? Jakie są ograniczenia Freesco?
Nie. A w zasadzie należałoby odpowiedzieć *na razie* nie. Freesco w założeniach jest systemem
pracującym z dyskietki. Jak wiemy nie uda nam sie zbyt wiele "upchnąć" na 1,4 MB. Pojemność dyskietki nakłada pewne ograniczenia. Stąd brak kompilera, obsługi systemu
plików CDROMU, dysków SCSI. I zapewne wielu innych przydatnych rzeczy. Jednak dzięki
rzeszy zapaleńców ten sytem wciąż się rozwija i obecnie już wiadomo, że trwają prace nad
przygotowaniem pakietów z kompilerem, Webminem, jest już pakiet z obsługą CDROMU (choć
na razie w wersji pre-alfa). Poza tym przy odrobinie wiedzy możemy nasze Freesco wyposażyć w potrzebne funkcje.

Inną przyczyną pewnych ograniczeń funkcjonalności Freesco jest stosunkowo stary kernel.
Freesco jest zbudowane na bazie jądra 2.0.38, obecnie mamy dostępne wersje 2.4.x (mówimy
tu o wersjach stabilnych). Niestety w związku z tym obsługa CBQ, ipchains, iptables, jest
niedostępna. Również niektóre programy wymagają nowszego jądra. Na pocieszenie należy
dodać, że trwają obecnie rozmowy nad nową, większą wersją Freesco - nazwa robocza to
FATSCO (fat - tłusty, gruby). Należy przypuszczać, że będzie ona wyposażona we wszystkie
nowinki... trzeba tylko trochę poczekać, jako że projekt jest jeszcze w fazie planowania...
Jest jeszcze jedno ograniczenie na które dość często skarżą się użytkownicy Freesco - brak
możliwości obsługi programu NetMeeting (przynajmniej w momencie pisania tego tekstu autorzy
nie znali ani jednego przypadku aby komuś udało się uzyskać pełną funkcjonalność NM
w sieci z obsługiwanej przez Freesco). Nie wynika to jednak z samego Freesco ale z trudnościami związanymi z obsługą protokołu, z którego korzysta NM.
8.2 Freesco nie spełnia moich wymagań/jest dla mnie za trudne/nie podoba mi się. Czy istnieją
alternatywne rozwiązania?
Oczywiście, stworzono wiele dystrybucji wyspecjalizowanych w obsłudze sieci. Niektóre z nich
jak Freesco pracują z dyskietki, inne wymagają twardego dysku lub CDROMU. Z pośród dyskietkowych
dystrybucji polecić można LIAP - Linux in a pillbox (Linux w pigułce czyli polopiryna, www.liap.eu.org), CoyoteLinux (www.coyotelinux.com), LRP (Linux Router Project - http://www.linuxrouter.org) i wiele, wiele innych. Żadna z minidystrybucji nie ma jednak
takiego potencjału (system pakietów rozszerzających możliwości naszego serwera) i łatwości
konfiguracji jak Freesco. Oczywiście jeśli wiemy co nieco o linuksie nasze możliwości są
większe, jednak nawet zupełny laik może "postawić" bezpieczny serwer używając właśnie
Freesco. Z "dużych" specjalizowanych dystrybucji można polecić e-smith (www.esmith.org)
czy ClarkConnect (www.clarkconnect.org). Ponieważ Linux jest systemwm sieciowym, więc
można wykorzystać każdą dystrybucję, różnica polega włściwie tylko na łatwości konfiguracji.

Niestety jednak przystosowanie dowolnej dystrybucji do pracy jako serwer sieciowy wymaga
nieco pracy i wiedzy... Pod tym względem Freesco jest o wiele mniej wymagające nadal jednak
oferując duże możliwości.
Czyli podsumowując: Freesco i tak jest najlepsze ;-).

9. KOMUNIKATY W LOGACH FREESCO

9.1 Co oznaczają komunikaty w logach typu "checksum failed"?
kernel: MASQ: failed TCP/UDP checksum from 194.237.107.43!
Informują o odrzuceniu przez jądro systemu pakietów w których została wykryta nieprawidłowa
suma kontrolna służąca do sprawdzania poprawności takiego pakietu. Nie należy się tym
przejmować o ile nie jesteśmy zalewani setkami takich pakietów na minutę.
9.2 Czemu wyświetlają się komunikaty nameda w logach?
named[721]: NSTATS 1013883718 1013188908 A=5650 PTR=2279 MX=8
Co godzinę named wyświetla w logach dwie linijki ze statystykami pracy, wyjaśnień symboli
trzeba szukać w dokumencacji BINDa
9.3 Jak interpretować komunikaty w logach o odrzuceniu przez firewal pakietu?
kernel: IP fw-in rej ppp0 TCP 206.253.182.49:2423 213.96.126.138:80
L=48 S=0x00 I=29597 F=0x0040 T=108
Komunikat firewalla mówi, że nasz modem (ppp0) odebrał pakiet typu TCP z komputera o IP
206.253.182.49 wysłany do nas z portu 2423 na nasz port 80 i na skutek naszych reguł ochrony
odrzucił pakiet odsyłając komunikat ICMP o odrzuceniu (reject) do nadawcy.

10. DODATKOWE MATERIAŁY

10.1 Instalacja pakietów z własnego serwera Freesco.
a) Ściąganie pakietów: nazwom pakietów odpowiadają ich pliki instalacyjne wg schematu:
pakiet.sh
pakiet.tgz
Naprzykład pakiet *ftpd* składa się z *ftpd.sh* i *ftpd.tgz* Należy ściągnać dane pliki z któregoś serwera przy pomocy np. wgeta pod Freesco albo Internet Explorera na windzie. W IE piszemy
np: *http://www.freesco.arx.pl/pakiety/ftpd.sh* i *http://www.freesco.arx.pl/pakiety/ftpd.tgz*
Jeśli chcesz wiedzieć jakie pakiety są dostępne na danym serwerze to możesz ściągnąć ich
listę np. *http://www.freesco.arx.pl/pakiety/packages.txt* w tym pliku, o ile ktoś go umieścił, jest opis wszystkich pakietów.
b) Kopiujesz pod windą potrzebne/wybrane pakiety prosto na dyskietkę.
c) Dyskietkę wsadzasz do komputera z Freesco i montujesz ją:
mount -t vfat /dev/fd0 /fd
d) Robisz katalog na pakiety i kopiujesz je tam:
mkdir /mnt/router/www/pakiety i
cp /fd/ /mnt/router/www/pakiety*
e) Zmieniasz właściciela katalogu i plików:
chown -R nobody /mnt/router/www/pakiety, oraz zmieniasz atrybuty plików
na "no execute": *chmod 644 /mnt/router/www/pakiety/**
f) Teraz już możesz instalować pakiety komendą:
installpkg http://localhost/pakiety/pakiet
np. *installpkg http://localhost/pakiety/ftpd*
Pamiętaj, że serwer http na Freesco musi być uruchomiony. Domyślnie tak jest ale można
go wyłączyć w setupie i wtedy nie będzie miał kto serwować plików instalacyjnych. Nazwę
katalogu "pakiety" oczywiście można sobie zmienić na dowolną inną.
Autor: Olek (olotest@poczta.onet.pl)

10.2 Dostęp do drugiej partycji.

Jaki dysk dla Freesco, oto jest pytanie. Jesli zamierzamy zastosować pliki startowe MsDOS
(lub innego dosa), na dysku zakładamy partycję FAT16 lub FAT32 (jesli nasz dos ją obsługuje).
FAT32 może utworzyć partycję primary (główną) dostosowaną do wielkoąci naszego dysku.
Inaczej będzie jeśli założymy FAT16 - maksymalna wielkość takiej partycji to 2GB, większy
dysk należy zatem podzielić na kilka partycji.
Jeśli chcemy uruchomić Freesco bez MsDOS musimy liczyć się z jeszcze jednym ograniczeniem.
System nie wystartuje na dysku 2GB z partycją FAT16. Przyczyną są klastry wielkości 32kB.
W moim przypadku zatrzymał się już po komunikacie *SYSLINUX...* Na grupie *trzepak.freesco*
mówiono o komunikatach, które informowały o nieobsługiwaniu klastrów większych niż
16kB.
Co zatem zrobić? Należy podzielić dysk na partycje w taki sposób, aby system umieszczony
został na partycji FAT16 o wielkości około 500 MB - tyle z powodzeniem wystarczy.
Zastosowałem podział na partycje i pierwszą przeznaczyłem na system, a drugą na katalog
/home (strony www i katalogi użytkowników). Dysk logiczny na partycji rozszerzonej montuję
wówczas komendą *mount -t umsdos /dev/hda5 /hd* lub *mount -t vfat /dev/hda5 /hd*. W
zależności od zastosowanego ramdisku i wielkości dysku, możemy mieć więcej niż dwie partycje
i te następne mogą mieć FAT32.
Jeśli chcemy korzystać na stałe z drugiej partycji we Freesco, musimy dokonać przystosowania
tej partycji, przez umieszczenie tam pliku odpowiedzialnego za przydzielanie praw i własności
plików. Tak wygląda procedura:

```
mkdir /mnt/home
mount -t vfat /dev/hdb1 /mnt/home
cat /dev/null > /mnt/home/--linux-.--- #nie zgub żadnej kreseczki!
umount /mnt/home
mount -t umsdos /dev/hdb1 /mnt/home
umssync /mnt/home
sync
```

I to juz wszystko, polecenie umssync skróci nam wszystkie długie nazwy windowsowych
plików (jeśli takie są), ale jest to sytuacja jednorazowa dotycząca istniejących na tej partycji
plików. Po tej operacji będą dostępne długie nazwy i wszelkie uprawnienia plików. Aby mieć
drugą partycję dostępną po starcie, umieścic należy w pliku *rc_user* polecenie montowania:

```
mount -t umsdos /dev/hda5 /mnt/home
```

Uwaga! przykłady katalogów pochodzą ode mnie, każdy może sam zadecydowac w jakim
katalogu będzie zamontowana jego partycja.

10.3 Ramdisk - główny obraz systemu plików.

Freesco jest systemem , w którym zasadnicza część systemu plików jest umieszczona w tzw.
ramdysku. Jeśli zmienimy plik ramdisk, możemy tym samym zmienić możliwości (a także
wymagania) systemu. Wiele udoskonaleń systemu polega na zmianie ramdisku.
Dla polskiego użytkownika Freesco doskonałym wyjściem jest używanie systemu plików autorstwa
Leszka Filipskiego - zalety to: polska klawiatura i dodanych kilka utilsów: df du mkdosfs
fdisk. Ponieważ ukazała sie paczka Dingetje z narzędziami do linuxowego systemu plików, dalsze
niezrealizowane pomysły Leszka straciły na znaczeniu. Nie mniej jednak każdy może sobie
przystosować ramdisk do własnych potrzeb. Nie jest to specjalnie trudne - jeśli mamy sprawny
system i zainstalowany mc - aby ułatwić i przyśpieszyc pracę. Należy zacząć od zrobienia kopii
zapasowej - kopiujemy ramdisk do innego katalogu. Nastepnie w katalogu /mnt należy wykonać
następujące polecenia:

```
mv ramdisk ramdisk.gz
gzip -d ramdisk.gz
losetup /dev/loop0 ramdisk
mkdir ram
mount -t ext2 /dev/loop0 ram
```

Uruchamiamy mc i w katalogu /mnt/ram znajdziemy zawartość ramdisku. Możemy wówczas
dodać aplikacje i edytować pliki. Należy to robic z dużą ostrożnością. Wielkość ramdysku nie jest
bez znaczenia dla pracy serwera, musimy być pewni, że serwer ma dostateczną ilość pamięci
RAM. Jeśli zamierzamy dodać np. kolejną partycję musimy w katalogu /mnt/ram/dev wydać
polecenie:

```
mknod hdc1 b 3 2 (hdc1 - to tylko przykład)
```

Jeśli zakończyliśmy pracę, opuszczamy katalog ram. Teraz odmontowujemy obraz i skopiować
na miejsce starego, wykonujemy polecenia odwrotne:

```
umount ram
losetup -d /dev/loop0
gzip ramdisk
mv ramdisk.gz ramdisk
```

Aby ułatwic sobie odzyskanie ramdisku w razie niepowodzenia, kopiujemy stary ramdisk do
katalogu /mnt pod nazwą ramdisk.old i robimy restart. Jeśli sie nie udało, uruchomic należy
Freesco z dyskietki, zamontować dysk komendą: *mount -t umsdos /dev/hda1 /hd* i przejśc do
odpowiedniego katalogu: *cd hd* - w tym katalogu wykonujemy komendę: *mv ramdisk.old ramdisk*
i restartujemy system, uruchamiając go z twardego dysku.
Opis ten powstał dzięki wskazówkom jakich udzielał mi Mis' i na podstawie postów L.Filipskiego
na grupie trzepak.freesco, które mi podesłał. Dziekuję za pomoc. Maciek (emti@and.pl)

10.4 Hardware - czyli na czym uruchamiać Freesco.
Ponieważ Freesco oparte jest na dosyc starym jądrze linuxa i przeznaczone do pracy jako jednodyskietkowy
router ma nie tylko ograniczone wymagania sprzętowe, ale również ograniczenia stąd wynikające. W zasadzie nie ma specjalnych problemów z płytami głównymi, ani kartami graficznymi czy dyskami. Udało mi się bez problemów uruchomić system na starym
486 z magistralą ISA, jak i na nowoczesnym Celeronie 1GHz z 256MB RAM z kartą graficzną
AGP i sieciową PCI...
Freesco spełnia rolę routera i serwera więc największą rolę odgrywają karty sieciowe i modemy.
Uczestnicy dyskusji na grupie *trzepak.freesco* są osobami, które wypróbowały wiele spośród kart sieciowych i na podstawie ich doświadczeń można spróbować zrobić listę kart
sieciowych, które nie sprawią problemów:
3COM 3C509 Combo ISA
D-Link DE-220 Family 16-bit ISA
zgodne z NE2000 ISA/PCI
3C503 ISA
ATI Realtek PCI 10/100
Compex RE 100TX 10/100 PCI Fast Ethernet Adapter
Intel Ethernet Express PRO 10/100 PnP
Planet ENW-9503/04 PCI
oraz karty na chipdsetach Realtek, karty Digitus Network.
Wszędzie tam gdzie wystarczy karta 10Mbit polecałbym sieciówkę zgodną z NE2000 ISA,
ponieważ istnieje przygotowany dla tych kart mniejszy niż standardowy plik *modules.tgz*, dzięki któremu system wczytuje się szybciej. Jeśli potrzebujemy sieci Fast Ethernet 100Mbit
dobrym rozwiązaniem będą karty Planet, które zresztą posiadają dyskietki ze sterownikami
(w tym do linuxa).
Freesco będzie bez problemów pracować z modemami zewnętrznymi podłączonymi do portu
COM1 lub 2 i ze sprzętowymi modemami wewnętrznymi. Winmodemy niestety są wykluczone,
a i pozostałe modemy PCI mogą sprawiać problemy.
Autor: Maciek (emti@and.pl)

10.5 Edycja plików tekstowych.
Brak Worda z wyskakującym na sprężynce elektronicznym idiotą, który rzekomo ma nam
podpowiadać, bedzie na pewno trudny do zrekompensowania dla miłośników Micro$oftu. Jednak
jest w naszym komputerze program, który pomoże nam w łatwy sposób edytować pliki
konfiguracyjne lub nawet pisać strony w htmlu czy php.
Jest to aplikacja *edit*, którą wywołujemy poleceniem: *edt /mnt/home/user/plik.txt*. Takie polecenie
wywołuje nam do edycji plik w katalogu */mnt/home/user*, nazwa pliku to *plik.txt* - jeśli taki nie istnieje, to zostanie utworzony. Polecenia programu są proste: F1 - pomoc, ALT+S
- zapisanie pliku, F10 - wyjście z programu. Strzałkami (w górę w dół) możemy poruszać się
wzdłuż wierszy tekstu. Więcej skrótów można znaleźć po naciśnięciu klawisza pomocy. Jeśli
zainstalowaliśmy sobie w naszym FREESCO *newram.gz* ze strony Leszka Filipskiego, to mamy
polską klawiaturę w standardzie ISO-8859-2, który obowiązuje w Internecie i możemy pisać
teksty, które będą potem poprawnie wyświetlane przez wszystkie przeglądarki internetowe.
Autor: Maciek (emti@and.pl)
10.6 Konsole wirtualne.
Domyślnie Freesco ma 2 konsole, na trzeciej wyswietlany jest raport systemu na czwartej
logowania użytkowników. Na piątej, jeśli zainstalowaliśmy, wyświetlany jest monitor *iptraf*.
Możemy dodać sobie jeszcze 2 konsole: *tty6* i *tty7*. W ten sposób do pracy będziemy mieli
cztery konsole wirtualne...
Należy dopisać w pliku *rc_init* po linii: *"fork daemon - "agetty 9600 tty2" &"* następną linię lub linie o identycznej treści zmieniając tylko numery konsoli na wyżej podane: tty6 i tty7.
Po restarcie bedziemy mogli przełączać się także na dodatkowe konsole używając klawiszy
Ctrl+Alt+F1-7.
Autor: Maciek (emti@and.pl)
10.7 Super-user i bezpieczeństwo.
Superużytkownik czyli root w linuxie może wszystko - nawet kompletnie rozłożyć serwer.
Dlatego należy korzystać z tego konta ostrożnie i z rozwagą, szczególnie we Freesco. W tym
systemie nie ma "kosza" - pliki znikają bezpowrotnie.

Warto sobie zatem utworzyć konta pomocnicze, np. *webadmin, ftpadmin* do administrowania
plikami na stronach www czy w katalogu ftp. Ponadto zbyt łatwe korzystanie z konta root
może byc potencjalnie niebezpieczne ze względu na możliwości włamań.
Przede wszystkim należy zrezygnować z telnetu, w którym hasła są przesyłane otwartym
tekstem. Wyłączamy tę usługę całkowicie w setupie. Należy do zdalnego logowania się zainstalować paczkę z SSH, jak to już odrębny temat, w pliku konfiguracyjnym wyłączyć rootowi
możliwość zdalnego logowania:
sshd_config - linia: PermitRootLogin no
No i root może się logować tylko na komputerze z Freesco. Jednak czasem możemy potrzebować
zdalnego logowania. W opcjach pliku rc_sshd możemy ustalić czy ma to być usługa dostępna
jedynie w sieci czy także z Internetu. Aby zyskać uprawnienia roota po zalogowaniu się jako
user, potrzebujemy aplikacji *su*. Komenda "*su*" powoduje zapytanie o hasło roota i przejmujemy
jego uprawnienia. Natomiast polecenie "*su - webadmin*", skutkuje zapytaniem o hasło *webadmina* i przejęcie jego uprawnień, oczywiście jesli mamy takie konto w systemie.
10.8 Zmiana hasła

Zmian hasła jest elementem, który we freesco jest niedopracowany. Poniżej kilka uwag jak
poradzić sobie z wyskakującymi przy tej czynności błędami. Niestety bez ręcznej roboty (czytaj:
grzebania w plikach) się nie obejdzie, ciężkie życie admina...
User nie może zmienić hasła w shellu - pojawią się dwa komunikaty: *can't open ptmp...* i *can't*
copy /etc/passwd to /mnt/router/etc...
Można temu zaradzić wpisując w pliku rc_user nadawanie plikowi */bin/passwd* bitu *SUID* wówczas
program wykonywany jest z prawami roota i zmiana hasła zacznie działać. Drugim sposobem
jest zainstalowanie pakietu *webpwd*, ale tu także mamy kłopot. Zakładam, że w systemie
jest zainstalowany pakiet Leszka Filipskiego *useradd*. W przeciwnym razie edycje userów
i tak musimy robic ręcznie, ponieważ oryginalny *adduser* z Freesco każdemu użytkownikowi
przypisuje ten sam numer, a to może być przyczyną innych problemów. A zatem co zrobić
aby można było korzystać z możliwości zmiany hasła z poziomu przeglądarki internetowej. Po
zainstalowaniu pakietu *webpwd* dodajemy nowego użytkownika do systemu.

Login name for new user []: ala
User id for ala [defaults to next available]:
Initial group for ala [users]:
Additional group for ala []: mail
ala's home directory [/mnt/home/ala]:
ala's shell [/bin/sh]:
OK, I'm about to make a new account. Here's what you entered so far:
New login name: ala
New UID: 504
Initial group: users
Additional group: mail
Home directory: /mnt/home/ala
Shell: /bin/sh
Expiry date: [no expiration]

Naciskamy ENTER i nadajemy hasło użytkownikowi. W następnej kolejności poddajemy edycji
plik */mnt/router/etc/passwd*, linia dodanego usera wygląda tak:
ala:PA/wsHG7E43:504:100::/mnt/home/ala:/bin/sh
i widzimy w niej dwa dwukropki, jest to miejsce na wpisanie "real name". Wpisujemy tam
nazwę usera między dwukropki:
ala:PA/wsHG7E43:504:100:ala:/mnt/home/ala:/bin/sh
w przeciwnym wypadku skrypt *webpwd* zlikwiduje nam jeden z dwukropków i na końcu dopisze
:(null) - hasło będzie zmienione, ale konto stanie się niedostępne.
Teraz jeszcze pozostaje sprawdzić działanie webpwd - wchodzimy na stronę i przeprowadzamy
zmianę hasła. Powinno zadziałać, u siebie musiałem jeszcze nadać bit SUID plikowi
newpasswd.cgi, czasmi też może będzie trzeba zrobić reboot, przed zadziałaniem metody.
Uwaga! Useradd także czasami myli numery i kolejnemu użytkownikowi przypisuje numer
1000, ten element także trzeba zmienić.