LTSP – sieć bezdyskowych terminali (część II)

Wilk w owczej skórze

Niezbyt nowoczesne komputery, które w wielu szkołach masowo oddawane są do wymiany, mogą posłużyć jako graficzne, wydajne terminale. Prezentujemy dokończenie artykułu z LM 7/2004, przedstawiającego wdrożenie LTSP w płockim Technikum Uzupełniającym dla Dorosłych SIMP.

RAJMUND RADZIEWICZ

W pakiecie *lts_x_core* znajdują się praktycznie wszystkie sterowniki kart wspieranych przez XFree86 w wersji 4.1. Jeśli zatem posiadamy taką kartę, z powodzeniem możemy to ustawienie zostawić bez zmian. Jeśli nie chcemy korzystać z opcji *auto*, możemy sami wpisać tutaj odpowiednią wartość, przykładowo *XSERVER = sis*.

Parametr X_MOUSE_DEVICE definiuje urządzenie, do którego podłączona jest mysz. Dla myszy PS/2 będzie to /dev/psaux. Gdybyśmy posiadali mysz szeregową, wpiszemy tutaj */dev/ttyS0* lub */dev/ttyS1*. X_VERTREFRESH to odświeżanie pionowe naszego monitora. Ustawienie *60* jest optymalną wartością, szczególnie dla starszych modeli. USE_XFS informuje, czy korzystamy z serwera czcionek. LOCAL_APPS to możliwość uruchamiania niektórych aplikacji lokalnie przez terminal. Jeśli ustawimy na Y, musimy skonfigurować w sieci serwer NIS i dopisać dwa kolejne parametry do lts.conf: NIS_DOMAIN, w którym wpiszemy nazwę domeny NIS oraz NIS_SERVER, gdzie wpiszemy jego adres. Zalecaną metodą jest oczywiście uruchamianie aplikacji na serwerze. Ponadto lokalne uruchamianie nawet niezbyt pamięciożernego programu wymaga już maszyny o trochę lepszych parametrach sprzętowych. XkbSymbols i XkbLayout to definicje klawiatury, natomiast RUNLEVEL oznacza poziom startowy naszych stacji. W LTSP standardowo mamy do dyspozycji poziomy: 3, 4 i 5. Poziom oznaczony numerem 3 uruchamia stacje w trybie tekstowym, poziom 4 oznacza sesję telnet, natomiast domyślnie ustawiony jest poziom 5. Jest to tryb graficzny, w którym po uruchomieniu każdy terminal (w tym wypadku można go już nazwać X-terminalem) pozwoli zalogować się do systemu za pośrednictwem uruchomionego na serwerze demona XDM, GDM lub KDM.

Ciekawą opcją LTSP jest możliwość korzystania z pliku wymiany. Informuje o tym parametr SWAPFILE_SIZE w sekcji przykładowego terminala *ws001*. Możemy utworzyć na serwerze plik wymiany dla naszych stacji, który będzie im udostępniony poprzez NFS. Domyślnie katalog */var/opt/ltsp/swapfiles* jest wówczas montowany jako */tmp/swapfiles*. Jeżeli nie mamy pliku wymiany, zostanie on utworzony automatycznie, a jego wielkość określi właśnie parametr SWAPFILE_SIZE. Plik wymiany może istnieć również na zupełnie innej maszynie w sieci. Jeśli taka sytuacja ma miejsce, musimy dopisać do naszego pliku *lts.conf* dodatkowy parametr SWAP_SERVER, w którym podamy adres tego komputera. Jeśli wszystko ustawiliśmy poprawnie, nie powinna nas w zasadzie spotkać żadna niemiła niespodzianka przy uruchamianiu stacji.

Uruchamianie terminala

Jeśli mamy już zainstalowane odpowiednie pakiety, ustawiony lts.conf i działające usługi DHCP, NFS oraz TFTP, możemy przejść do uruchamiania stacji roboczych. Do tego celu wykorzystamy narzędziem o nazwie Etherboot. Służy ono do tworzenia obrazów ROM, na których umieszczany jest specjalny program umożliwiający uruchomienie komputera przez sieć. Możemy co prawda zaopatrzyć się w karty sieciowe, które są już wyposażone w tzw. bootromy i wówczas nasze terminale przy każdym starcie będą domyślnie próbowały uruchomić się przez sieć i uzyskać dane od rozgła-

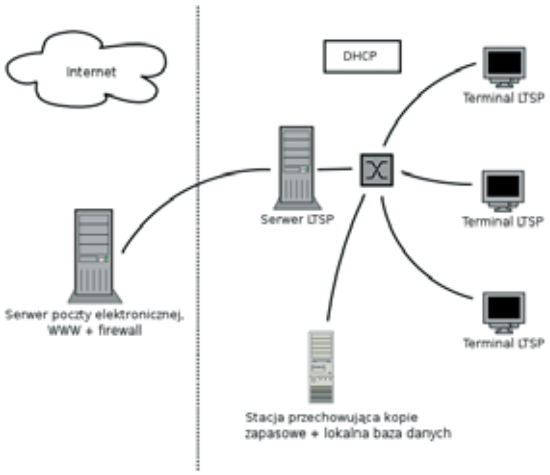
ZROBIMY TO W NUMERZE 9/2004...

KILL BILL

nie przegap!

LINUX MAGAZINE

szającego się serwera DHCP. Jako że jednak nie wszystkie starsze komputery, przeznaczane na terminale LTSP, posiadają takie karty, możemy wygenerować dyskietkę z bootrom-em, za pomocą której uruchomimy stacje. Ze strony *http://www.rom-o-matic.net* powinniśmy pobrać plik odpowiadający chipsetowi naszej karty sieciowej. Należy nagrać go na dyskietkę, np. poleceniem *cat plik.lzdsk > /dev/fd0*, i uruchomić za jej pomocą terminal. W BIOS terminala kolejność uruchamiania napędów powinna być oczywiście tak ustawiona, żeby w pierwszej kolejności sprawdzany był napęd dyskietek.



Rysunek 1: Schemat sieci opartej o LTSP w płockim Technikum Uzupełniającym dla Dorosłych SIMP.

Jeśli posiadamy starszy komputer, bez twardego dysku i napędu CD-ROM, zadanie to staje się wręcz jedyną możliwością. Dyskietka nie będzie oczywiście potrzebna przez cały czas pracy terminala. Kiedy ten komputer zainicjuje już program rozruchowy, otrzyma adres od serwera DHCP i zacznie ściągać jądro – możemy śmiało wyjąć ją z napędu i uruchamiać już kolejne maszyny (o ile oczywiście posiadają taką samą kartę sieciową). Jeżeli w lts.conf ustawiliśmy *RUNLEVEL* na 5, po chwili powinien uruchomić się tryb graficzny. Stacja robocza przekaże zapytanie do demona logowania na serwerze przy pomocy wspomnianego już XDMCP i wyświetli znajome okienko GDM, KDM lub XDM, w zależności od tego, z jakiego środowiska korzystamy. W przypadku Linux-EduCD jest to KDM. Logujemy się oczywiście na konto, które musi istnieć na serwerze.

Jeśli po uruchomieniu terminala serwer X nie chce się uruchomić, a jedynie restartuje co chwila ekran i ostatecznie zostaje w trybie tekstowym, należy sprawdzić ustawienia w lts.conf, w szczególności opcję XSERVER. Często przy słabszych kartach i monitorach, które nie potrafią uruchomić się w rozdzielczości 1024x768, wystarczy dopisać do sekcji terminali:

```
X_MODE_0 = 800x600
```

Jeśli po uruchomieniu i pomyślnym wystartowaniu serwera X na terminalu mamy jedynie szare tło i kursor na jego tle (nie uruchamia się KDM) – najczęściej oznacza to problemy z protokołem XDMCP. Należy sprawdzić wówczas, czy w pliku /etc/kde/kdm3/kdmrc mamy odkomentowany wpis:

```
[XDMCP]
Enable = true
```

To wszystko, jeśli chodzi o samodzielną instalację i uruchamianie LTSP. W przypadku dystrybucji Linux-EduCD oprogramowanie jest już zaimplementowane, więc przy konfiguracji sieci w płockim technikum większość z tych kroków można było pominąć. Wszystkie dostępne chipsety kart sieciowych, potrzebne do wygenerowania dyskietek, znajdują się w katalogu: /opt/bootroms. Dystrybucja pozwala na uruchamianie LTSP nawet podczas pracy z płyty CD, jednak zalecane jest oczywiście korzystanie z tego oprogramowania już po instalacji na dysku. Po zainstalowaniu na dysku Linux-EduCD otrzymujemy wstępnie skonfigurowany, oparty na Debianie system, który pracuje oczywiście dużo szybciej i wydajniej niż w przypadku działania z płyty. Po instalacji systemu operacyjnego na serwerze i założeniu odpowiedniej ilości kont ustawione zostały wspomniane opcje w pliku konfiguracyjnym lts.conf. Terminale w sieci to jedenaście jednakowych pecetów o parametrach AMD-K6 200 Mhz i 8 MB RAM. Wyposażone są w karty graficzne S3 Virge i karty sieciowe na chipsecie Realtek 8139. Poza napędem dyskietek, nie posiadają ani CD-ROM-ów, ani twardych dysków.

W Linux-EduCD LTSP nie uruchamia się domyślnie. Żeby to zrobić, należy uruchomić skrypt *start_ltsp*, do którego dowiązanie znajduje się w katalogu domowym użytkownika root. Istotne jest to, że pierwsze (i wyłącznie pierwsze) uruchomienie, wprost po instalacji dystrybucji na dysku, należy zainicjować innym skryptem – *hdd_ltsp*. Usługę możemy w dowolnej chwili zatrzymać, wykonując z kolei *stop_ltsp* lub wybierając z menu KDE opcję LTSP -> Zatrzymaj LTSP. Wszystkie wspomniane

Listing 1: Przykładowe reguły iptables dla LTSP

```
iptables -F
iptables -A INPUT -i lo -p all -j ACCEPT
iptables -A OUTPUT -o lo -p all -j ACCEPT
iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT – Akceptowanie połączeń nawiązanych
iptables -A INPUT -p tcp --tcp-option! 2 -j REJECT --reject-with tcp-reset
iptables -A INPUT -p tcp -i eth0 --dport 21 -j ACCEPT – Otwieramy port FTP
iptables -A INPUT -p udp -i eth0 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT – Otwieramy port SSH
iptables -A INPUT -p udp -i eth0 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT – Otwieramy port HTTP
iptables -A INPUT -p udp -i eth0 --dport 80 -j ACCEPT
iptables -P INPUT DROP – Domyślnie reszta jest blokowana
```

skrypty znajdują się w katalogu /opt, a ich dowiązania w /root.

W pliku start_ltsp znajdują się w zasadzie polecenia uruchamiające takie usługi jak: DHCP, NFS, portmap i KDM, czyli dokładnie to, co jest potrzebne do zaistnienia komunikacji pomiędzy serwerem a stacjami roboczymi. W pliku /etc/exports zdefiniowane są wymagane zasoby. W LinuxEduCD zawartość tego pliku wygląda następująco:

```
/opt/ltsp/i386 ➥
192.168.0.0/255.255.255.0➥
(ro,no_root_squash,sync)
/var/opt/ltsp/swapfiles ➥
192.168.0.0/255.255.255.0➥
(rw,no_root_squash,async)
/home 192.168.0.0/255.255.255.0➥
(rw,no_root_squash,sync)
```

Powyższe opcje w zupełności wystarczają do sprawnego udostępniania głównego drzewa katalogów dla terminali, pliku wymiany (o ile jest stosowany) i katalogów domowych. Możemy analogiczne wpisy ustawić także w przypadku instalacji LTSP w innym systemie.

Firewall

W zasadzie najbardziej optymalna konfiguracja serwera terminali to taka, w której ten stoi już za firewallem i sam nie udostępnia takich usług jak WWW, SMTP czy też DNS. Taki układ ma miejsce w przypadku płockiej sieci. W momencie, kiedy jednak to on jest bramą sieciową dla pozostałych komputerów, warto pamiętać, by poza maskaradą odpowiednio ustawić reguły filtrowania pakietów. Wskazane jest, żeby wymagane przez LTSP demony – NFS, portmap i inne, mogące stanowić potencjalną lukę w bezpieczeństwie systemu, nie były dostępne z zewnątrz.

Konfigurację firewalla możemy przeprowadzić na dwa sposoby. Jako że popularniejszy w nowszych wersjach jądra jest iptables – posłużymy się właśnie nim. Pierwszy sposób to blokowanie określonych portów przez dodawanie kolejnych reguł odrzucających pakiety:

```
iptables -A INPUT -p tcp -s 0/0 ➥
-d 0/0 --dport 2049 -j DROP
iptables -A INPUT -p udp -s 0/0 ➥
-d 0/0 --dport 2049 -j DROP
```

Powyższe reguły blokują np. port 2049 dla tcp i udp, wykorzystywany przez NFS. Posługując się taką metodą, będziemy musieli dla każdego portu, który chcemy zablokować, zdefiniować analogiczny wpis. Można też zastosować inną politykę – domyślnie blokować wszystkie pakiety i dodawać reguły dopuszczające tylko poszczególne usługi (patrz Listing 1).

Czasami zbyt restrykcyjnie zdefiniowane reguły mogą zablokować potrzebną do działania usługę (np. serwer DHCP). Po włączeniu reguł możemy w każdej chwili wyświetlić zastosowane zasady filtrowania pakietów poleceniem *iptables -L -v*.

Poniżej przedstawiam kilka przydatnych sposobów na ułatwienie pracy administratora w opisywanej sieci terminali, są to: tworzenie kopii zapasowych, wsadowe zakładanie kont użytkowników, kontrola procesów oraz korzystanie z lokalnych napędów dyskietek na stacjach roboczych. Oczywiście możliwości jest wiele więcej, wszystko zależy od wymagań i potrzeb.

Kopie zapasowe

Niezbędną czynnością w sieci, w której terminale pracują jako stacje robocze, jest rzecz jasna wykonywanie kopii zapasowych. Pomimo że dane składowane są w zasadzie wyłącznie na dysku serwera LTSP, wskazane jest, aby tym bardziej dbać o ich bezpieczeństwo. W przypadku płockiego technikum okresowo uruchamiany jest prosty skrypt, który wykonuje kopie katalogów domowych wszystkich użytkowników, archiwizuje je do /opt/kopie_zapasowe i przesyła na oddzielny komputer w sieci o adresie 192.168.1.10. Na komputerze tym, w katalogu /opt, znajduje się podkatalog *terminale_kopie*, do którego wędrują spakowane paczki. Nie jest to oczywiście wykonywanie kopii przyrostowych, a jedynie prosty sposób na pełne zarchiwizowanie danych. Skrypt kopiuje całą zawartość katalogów domowych, poza katalogiem *tymczasowe*. Jeśli użytkownicy mają jakieś mało istotne dane, które nie muszą być archiwizowane, mogą umieszczać je właśnie w tym katalogu (patrz Listing 2).

Listing 2: Skrypt tworzący kopie zapasowe katalogów domowych

```
#!/bin/bash
# najpierw tworzymy katalog
/opt/terminale_kopie na zdalnym
hoście

mkdir /opt/kopie_zapasowe
cd /home
users=`ls`
for x in $users
do
tar zcvf /opt/kopie_zapaso-
we/${x}.tgz /home/${x} --exclu-
de=tymczasowe
done

scp -r /opt/kopie_zapasowe
192.168.1.10:/opt/terminale_kopie
```

Jeśli istnieje potrzeba wykonywania kopii przyrostowych, należy synchronizować zawartość zdalnego */opt/terminale_kopie* z lokalnym */opt/kopie_zapasowe*. Można posłużyć się w tym celu programem rsync. W przeciwieństwie do programu tar, rsync przesyła zmiany, jakie zaszły od czasu wykonania ostatniej kopii. Polecenie:

```
rsync -ave ssh 192.168.1.10:/➥
opt/terminale_kopie/ /opt/➥
kopie_zapasowe/
```

powoduje, że kopia przed wysłaniem będzie odpowiednio zsynchronizowana.

Wsadowe tworzenie kont użytkowników

Wbrew pozorom, zakładanie kont systemowych w szkolnej pracowni wcale nie musi być sprawą łatwą. Przy założeniu, że z pracowni ma korzystać np. pięć średniej wielkości klas, a każdy uczeń ma mieć własne konto, wychodzi nam przynajmniej setka użytkowników. Oczywiście wpisywanie dla każdego konta polecenia *useradd* i dwukrotne powtarzanie hasła nie jest najciekawszym rozwiązaniem w takiej sytuacji. Z pomocą może nam przyjść program *newusers*. Służy on do wsadowej aktualizacji i tworzenia kont nowych użytkowników. Wystarczy, że dysponujemy listą zawierającą pary: użytkownik:hasło, dopiszemy do każdej linii informacje na temat katalogu domowego i możemy jednym poleceniem załatwić resztę „formalności”. Hasło powinno być podane jawnym tekstem, ponieważ newusers sam zajmie się jego zaszyfrowaniem. Na serwerze technikum użyliśmy listy *users* z wpisami:

```
uczen1:password::::/home/uczen1:
testowe1:password2::::/home/➥
testowe1:
```

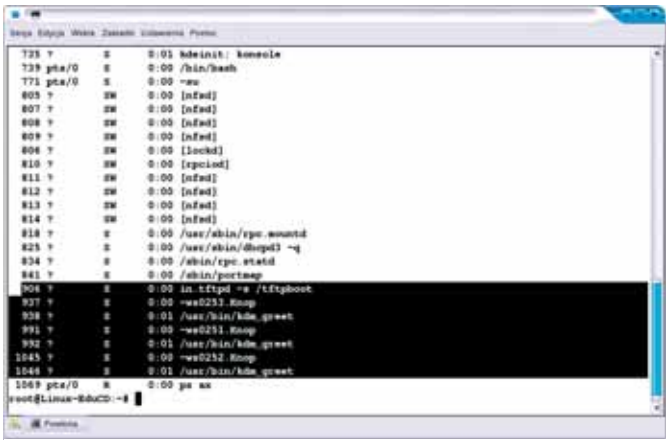
Należy pamiętać o odpowiedniej ilości znaków:. W zasadzie format tego zapisu jest analogiczny do wpisów w /etc/passwd. Jeśli lista jest gotowa, wykonujemy polecenie *newusers users*.

Po chwili konta są już założone, a za pomocą polecenia chpasswd można aktualizować zbiorowo hasła.

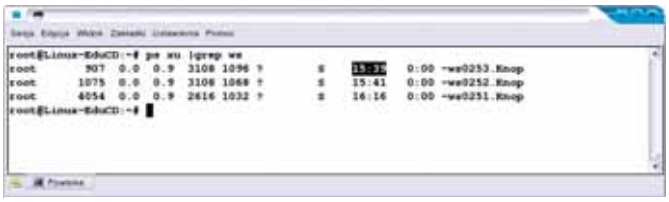
Udostępnianie lokalnych napędów dyskietek

Żeby umożliwić korzystanie na terminalach z lokalnych napędów dyskietek, niezbędny będzie pakiet mtools. Jest to zestaw narzędzi zapewniający dostęp do systemów plikowych DOS. Jeśli w systemie, w którym konfigurujemy LTSP, działa on na domyślnych ustawieniach zdefiniowanych w /etc/mtools.conf, można korzystać z napędu poprzez polecenie: *mdir a:*. Działa ono na napędzie, bez potrzeby wcześniejszego montowania czy też odmontowania. W dystrybucjach Debian, Knoppix, Linux-EduCD i innych mtools jest już zainstalowany, a plik /etc/mtools.conf zawiera odpowiednie dyrektywy.

Potrzebujemy jeszcze pakietu *ltsp_floppyd*. W chwili pisania artykułu, najnowszą jego wersją jest 3.0. Pobieramy więc ze strony projektu plik ltsp_floppyd-3.0.tar.gz, rozpakowujemy go i jako użytkownik root uruchamiamy skrypt *install_floppyd*. Teraz w sekcji poszczególnych terminali (lub w sekcji *Default*) pliku lts.conf ustawiamy opcję:



Rysunek 2: Na serwerze widoczne są procesy terminali i usług LTSP, w tym tftpd w trybie chroot.



Rysunek 3: Za pomocą polecenia *ps* możemy również sprawdzić, o której dokładnie godzinie terminal został uruchomiony.

```
RCFILE_01 = floppyd
```

Następnie w katalogu każdego użytkownika, który ma mieć dostęp do lokalnego napędu dyskietek, tworzymy ukryty plik *.mtoolsrc* z wpisem:

```
drive a: file='$DISPLAY' remote
1.44m mformat_only
```

Po tej czynności możemy uruchomić terminal i zalogować się na konto użytkownika, w którego katalogu domowym znajduje się plik .mtoolsrc. Można też za pomocą polecenia *mdir a:* spróbować pokazać zawartość dyskietki.

Automatyczne wylogowanie

Wszystkie aplikacje i procesy uruchamiane przez terminale rezydują na serwerze. Daje to dużą kontrolę nad wszelkimi działaniami użytkowników. W momencie kiedy są zalogowani, możemy sprawdzać, jak długo pracują i z jakich korzystają aktualnie programów. Wiemy, że w /etc/hosts nasze terminale nazwane są kolejno: ws001, ws002. Wystarczy więc przefiltrować odpowiednio procesy, żeby sprawdzić, ile takich terminali aktualnie pracuje:

```
ps ax | grep ws
```

Możemy w analogiczny sposób sprawdzić, jakie aplikacje są wykorzystywane oraz czy pracują wszystkie usługi odpowiedzialne za LTSP.

Użytkowników możemy wylogować z serwera w każdej chwili, posługując się prostym skryptem i nazwą użytkownika, podaną jako parametr. Skrypt o nazwie *wyloguj* znajduje się na Listingu 3.

Po utworzeniu takiego skryptu należy oczywiście nadać mu atrybut wykonywalności. Jeśli zalogowany jest np. użytkownik *rajmund*, wystarczy jako root wykonać polecenie:

```
./wyloguj rajmund
```

LTSP jest z pewnością bardzo użytecznym oprogramowaniem. Sprawdza się znakomicie jako niezwykle wydajny system terminali, drobiazgowo przemyślany zarówno pod kątem funkcjonalności, jak i łatwości obsługi. Po więcej szczegółowych informacji odsyłam do oficjalnej dokumentacji. ■

Listing 5: Skrypt pomocny przy wylogowaniu użytkowników LTSP

```
#!/bin/sh
# skrypt do wylogowania użytkowników LTSP

if [ $1!= 'root' ]
then
 for i in $(pgrep -u $1)
 do
 kill -9 $i
 done
 else
 clear
 echo 'Nie można zabić sesji roota'

 fi
```

INFO

[1] Strona projektu LTSP: *http://www.ltsp.org*

[2] Strona projektu Etherboot: *http://www.rom-o-matic.net*

[3] Dystrybucja Linux-EduCD: *http://www.simp-st.pl*