WIESŁAW M. TRĄMPCZYŃSKI

PODRĘCZNIK UŻYTKOWNIKA

© 2009 W.T.

Spis treści

Projekt EOS – założenia ogólne....3
Bardzo ogólnie....3
Bardziej szczegółowo....3
Zalety i Wady....4
Dodatkowe informacje....4
Instalacja i konfiguracja serwera....5
Instalacja....5
Sprzęt....5
Uruchamianie z płyty....5
Pierwsze uruchomienie....7
Konfiguracja ADSL....9
Inne typy połączeń sieciowych....11
Konfiguracja komputera i usług....11
Zegar i strefa czasowa....11
Dansguardian i Squid....11
Konfiguracja....12
Zarządzanie MySQL....13
Zmiana domyślnego hasła....13
Zarządzanie serwerem www i Moodle....14
Konfiguracja poczty....16
Konfiguracja Exima....16
Administracja użytkownikami....17
Konfiguracja firewalla....19
Podstawowe ustawienia....19
Przekierowanie portów....20
System narzędziowy z PXE....21
Konfiguracja drukarki sieciowej....23
Samba....26
NIS i NFS....26
Serwer FTP....27
Ochrona antywirusowa....27
Fail2ban....28
Instalacja i konfiguracja stacji roboczej....29
Windows....29
Linux....30
Uruchomienie z płyty DVD....30
Instalacja na dysku....31
Pierwsze uruchomienie....33
Interesujące dodatki....35
Kontrola stacji programem iTALC....35
Instalacja i konfiguracja....35
Zarządzanie....37
Statyczne wpisy DHCP....39
Zdalny dostęp do serwera....39
Aplikacje administratora....43
Rozwiązywanie problemów....49
O dokumencie....50

Projekt EOS – założenia ogólne

Bardzo ogólnie...

Idea prostego i łatwego serwera dla szkolnej pracownie nie jest nowa. Założenia te miały spełnić dotychczasowe projekty, jednak okazało się, że praktyka przeczy założeniom. Szczególnie trudne w administrowaniu okazały się najpopularniejsze w kraju zestawy z zainstalowanym systemem firmy *Microsoft*.

W wielu szkołach nauczyciele, nie radząc sobie z oprogramowaniem, rezygnowali z serwera. Łączyli komputery w sieć równorzędną, co również nie było dobrym pomysłem. W takim przypadku nie ma mowy o kontroli nad poczynaniami uczniów, łatwiej o zainfekowanie komputerów złośliwym oprogramowaniem i trudno w ogóle mówić o pracy zdalnej, czy zasobach współdzielonych.

Projekt **EOS** ma za zadanie przedstawić alternatywę dla obecnie istniejących szkolnych pracowni. Pracownia ma być łatwa w instalacji i konfiguracji i możliwie najbardziej stabilna. Musi też spełniać warunki bezpiecznej pracy w sieci. System powinien też umożliwiać pracę w sieci heterogenicznej. **EOS** ma wszelkie zalety do zastosowania również w innych niewielkich sieciach – w charakterze routera lub serwera internetowego.

Bardziej szczegółowo...

Serwer

Podstawą systemu jest dystrybucja *PCLinuxOS*, której motto brzmi „Radically Simple" (radykalnie prosty). Aby system umożliwiał logowanie klientów używających *Windows* i *Linuksa*, zastosowano podwójny mechanizm. NIS (*Network Information Service*) sprawdza użytkowników linuksowych, a korzystających z *Windows - Samba*, będąc jednocześnie serwerem autoryzacji haseł dla obu grup użytkowników. Pozwala to uniknąć dublowania kont i w przypadku stacji z obydwoma systemami umożliwia uczniowi pracę na jednym koncie. Jest to rozwiązanie bardzo proste i niezawodne. Mechanizm udostępniania zasobów serwera dla systemów *Windows* to *Samba*, a dla klientów linuksowych – NFS (*Network File System*). Ponadto serwer wyposażony jest w prosty i skuteczny firewall oraz podstawowy mechanizm dynamicznego dzielenia łącza.

Zgodnie z zaleceniami MEN, dostęp do internetu odbywa się przez serwer proxy wyposażony w mechanizm filtrowania niepożądanych treści (*Squid* oraz *Dansguardian*). Jedną z ważniejszych funkcji, według sugestii nauczycieli, jest możliwość używania platformy zdalnego nauczania – *Moodle*. Dlatego też zainstalowany jest serwer *Apache* ze wsparciem dla PHP5 i MySQL. Mechanizm *Moodle* został wstępnie skonfigurowany.

Konfigurację podstawową przeprowadza się przy użyciu dostępnych narzędzi systemowych, zaś konfigurację usług serwerowych kilkoma dodatkowymi skryptami.

System *Linux* ma jedną bardzo istotną zaletę, w razie potrzeby łatwo znaleźć dodatkowe potrzebne oprogramowanie, które będzie można zainstalować kilkoma kliknięciami. W miarę rozwoju projektu i potrzeb zgłaszanych przez nauczycieli będzie możliwe wyposażanie serwerów w dodatkowe programy i narzędzia. Istotną zaletą serwera **EOS** jest nie tylko łatwość i szybkość przystosowania do pracy w szkolnej pracowni, ale również możliwość skonfigurowania do pracy wersji Live.

Stacja robocza

W założeniu stacje robocze mogą korzystać z systemu *Windows* i zapewne będzie to opcja, z której skorzystają szkoły zamierzające zmienić obecny serwer, a pozostawić system dotychczasowy na komputerach klienckich. Tam, gdzie nauczyciele zdecydują się korzystać ze stacji linuksowych, można zainstalować z obrazu stację **EOS**. System stacji

zawiera oprogramowanie, które może być przydatne w różnych typach szkół. Pierwsza grupa programów – dla szkół podstawowych, skupia się na uczynieniu z informatyki przedmiotu ciekawego w myśl zasady" „Uczyć bawiąc, bawić ucząc." Osią główną stają się tu gry i zabawy o charakterze edukacyjnym z suitą *Gcompris* na czele. Oprócz tego jest również oprogramowanie medialne, internetowe i biurowe. W gimnazjum nacisk większy będzie na programy biurowe, graficzne i medialne, a także na oprogramowanie pozwalające na wykonywanie rozmaitych projektów grafiki wektorowej, nauki DTP i zaawansowane korzystanie z internetu. W szkołach średnich oprócz oprogramowania już wymienionego, będą również zapewne używane aplikacje do projektowania np. Qcad. W gimnazjach i szkołach średnich można również zainstalować środowisko programistyczne.

Zalety i Wady

Do zalet niewątpliwie należy prostota instalacji i konfiguracji systemu, zarówno na serwerze, jak i na stacji roboczej. W sytuacji permanentnego niedofinansowania szkół duże znaczenie maja koszty. W przypadku **EOS** mogą być one bardzo niewielkie, ponieważ ograniczą się jedynie do położenia sieci i wdrożenia (w przypadku nowej pracowni). Koszty serwisowania pracowni w praktyce sprowadzają się do serwisu sprzętowego.

Pewną wadą jest z góry założona konfiguracja, której zmiana wcale już nie będzie taka prosta. Jednak należy pamiętać, że identycznie skonfigurowane są wszystkie pracownie szkolne – te z *Windows*, z komputerami *Apple* i z serwerem *Novell*, a także linuksowe. Kolejna wada, to brak opcji instalacji zdalnej. Technicznie jest to możliwe do wdrożenia, lecz ze względów licencyjnych nie jest możliwe rozpowszechnianie obrazu stacji *Windows*. Jednak nauczyciel taką odmianę usługi *RIS* może sam wdrożyć. Instalacja sieciowa stacji linuksowej jest możliwa i być może w przyszłości zostanie to dodane.

Dodatkowe informacje

Obecną wersję 2009 można określić jako w pełni działająca finalną. Poprawiono wszystkie znane błędy wersji beta. Poprawki, które będą dokonywane, to głównie udoskonalanie skryptów konfiguracyjnych i będą mogły być zainstalowane w formie pakietów. Jest podstawowy obraz serwera i stacji roboczej. Obecnie projekt wymaga przetestowania w realnych warunkach pracowni szkolnej, w celu wyeliminowania problemów, jakie się mogą pojawić.

Dlaczego **EOS**? W mitologii greckiej *Eos* (*Jutrzenka*, *Świt*) to bogini rozpoczynająca nowy dzień. Poranek to zawsze chwila nadziei, że będzie lepiej. **EOS** to także akronim słów Educational Operating System.

Niniejszy dokument zawiera opis instalacji, konfiguracji oraz pracy na serwerze oraz stacji roboczej **EOS**. Informacje na temat działających na serwerze usług są ograniczone do niezbędnych wskazówek konfiguracyjnych i z pewnością nie wyczerpują tematu, z tego względu użytkownik zainteresowany wdrożeniem innych niż podstawowe funkcji, powinien szukać bardziej obszernych informacji. Główne rozdziały poświęcone są instalacji i konfiguracji systemu oraz najważniejszym aspektom codziennej pracy. W razie problemów należy szukać rozwiązań w rozdziale „Rozwiązywanie problemów", w którym zostały opisane najczęstsze przyczyny niepowodzeń w uruchamianiu, bądź konfigurowaniu systemu.

Uwaga! Powyższy znak będzie umieszczony przy opisie konfiguracji usług, które nie są przeznaczone dla osób początkujących.

Instalacja i konfiguracja serwera

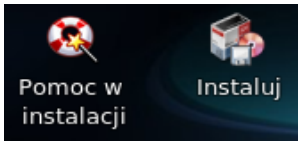
Instalacja

Sprzęt

Minimalne wymagania sprzętowe dotyczą głównie pamięci. Podstawowe minimum to 512 MB, Jednak normalna praca i działanie wszystkich usług (w tym *Apache* z zainstalowanym *Moodle*) wymagają przynajmniej 1 GB RAM. Pewność komfortowej pracy da posiadanie 2 GB pamięci operacyjnej. Procesor powinien mieć taktowanie co najmniej 1,6 GHz. Każdy z obecnie produkowanych procesorów dwurdzeniowych będzie odpowiedni. Karta graficzna nie jest kluczowa dla działania systemu jednak najlepsze będą karty na chipsetach *Nvidia*® lub *Intel*®. System poprawnie wykryje prawie wszystkie karty dźwiękowe oprócz może tych najstarszych. Potrzebny będzie dowolny napęd DVD i twardy dysk. Sam system zajmie początkowo nie więcej niż 4 GB, jednak podczas pracy będą tworzone katalogi i pliki użytkowników, więc lepiej dysponować dyskiem o pojemności co najmniej 80GB.

Uruchamianie z płyty

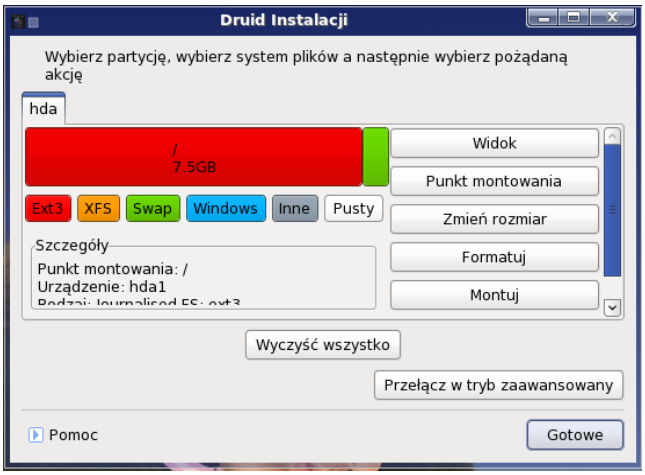
Jeśli komputer nie startuje automatycznie z płyty DVD, trzeba zmienić opcję uruchamiania w BIOSie komputera. Przed zalogowaniem pojawia się okno wyboru klawiatury. Wybieramy klawiaturę *„polski (programisty)”*.Po uruchomieniu systemu i zalogowaniu się (użytkownik *guest* z hasłem *guest*), należy zainstalować system na twardym dysku. Na pulpicie znajdują się ikony, jedna do programu instalacyjnego, a druga otwierająca plik pomocy(*Rysunek 1: Ikony na pulpicie*). Należy przeczytać instrukcję i pozostawić ją otwartą podczas procesu instalacji, ponieważ zawarte tam informacje mogą się przydać.



Rysunek 1: Ikony na pulpicie

Kliknięcie ikony *Instaluj* spowoduje pojawienie się pytania o hasło roota (hasło *root*). Pierwsze pytanie będzie dotyczyć usunięcia zwykle nieużywanych sterowników zamkniętych do kart graficznych. Należy je usunąć, gdy nie mamy kart *ATI* lub *Nvidia*, choć nie jest to konieczne. Następnie pojawi się okno kreatora dysku. Należy pominąć ostrzeżenie o konieczności zarchiwizowania danych na dysku, jeśli jesteśmy pewni, że chcemy system zainstalować. W zależności od sytuacji, kreator wykryje dysk (lub dyski) i pozwoli wybrać oraz odpowiednio przygotować partycje. Najlepiej zawsze wybrać możliwość ręcznego przygotowania dysku, będziemy pewni, że nad wszystkim panujemy (*Rysunek 2: Okno ręcznego podziału dysku na partycje*).

Zaleca się utworzenie partycji głównej (/) większej niż minimum. Użytkownik będzie miał możliwość utworzyć własną płytę jako kopię zapasową systemu po przeprowadzonej konfiguracji, więc na partycji systemowej powinno być kilka gigabajtów więcej niż zajmuje system. Należy utworzyć drugą partycję na dane użytkowników (/home) i na nią przydzielić pozostałą część dysku. Partycję swap warto utworzyć w wielkości odpowiadającej pamięci RAM.

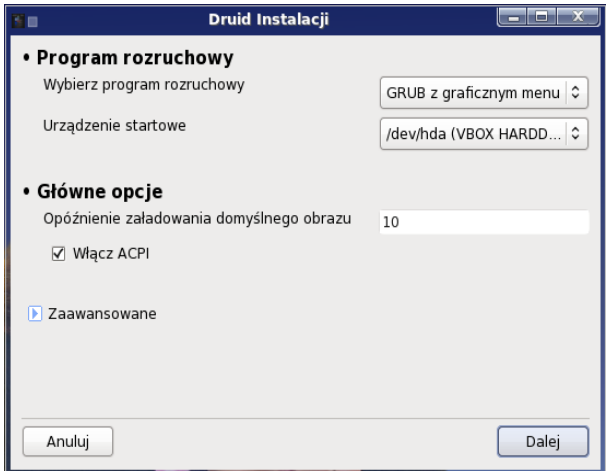


Rysunek 2: Okno ręcznego podziału dysku na partycje

W zależności od posiadanego dysku można wybrać różne sposoby jego podziału (*Rysunek 3: Przykładowy podział dysku*). Podział partycji i rozmiary dobrze jest sobie zaplanować przed podjęciem instalacji. Można rozważyć wydzielenie osobnych partycji nie tylko na */home* ale i na */var*.

Rysunek 3: Przykładowy podział dysku

Po kilkunastu minutach nastąpi jeszcze moment instalacji bootloadera (inaczej mówiąc menedżera startu) i należy zrestartować komputer. Należy pozostawić domyślne opcje, ponieważ instalator zwykle bez problemu wykryje również inne zainstalowane systemy (*Rysunek 4: Okno instalacji programu rozruchowego*). Później można zmienić sobie również tzw. etykietę, co zostało opisane w końcowej części podręcznika.



Rysunek 4: Okno instalacji programu rozruchowego

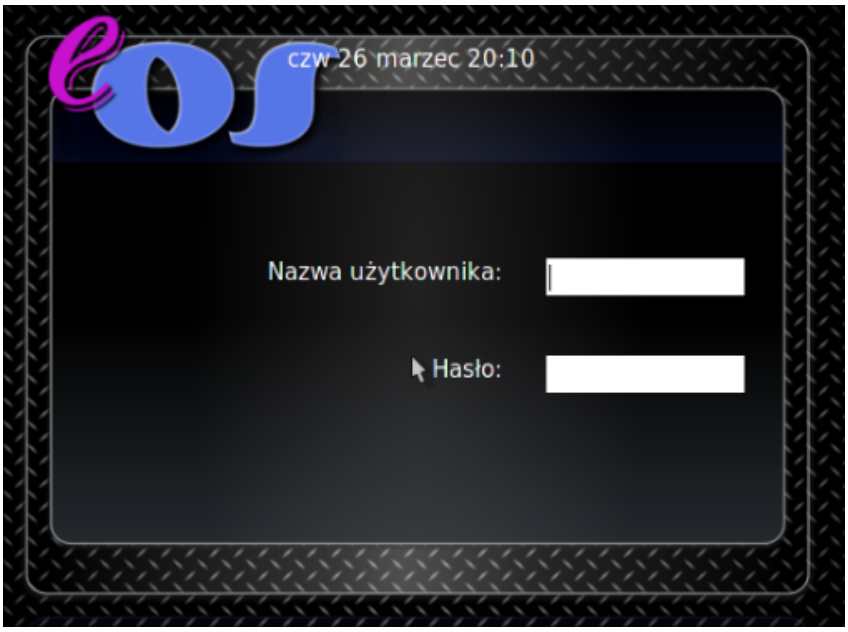
Mając 1 GB pamięci RAM można zupełnie normalnie używać systemu w wersji *Live*, bez efektu spowolnienia działania. Można również skonfigurować i uruchomić sieć oraz wszystkie zainstalowane usługi, aby w ten sposób sprawdzić, czy wszystko działa w naszej sieci poprawnie. Instalację na dysku należy jednak przeprowadzić bez konfiguracji na świeżo uruchomionej wersji *Live*.

Pierwsze uruchomienie

Po instalacji podczas pierwszego uruchomienia pojawi się okno ustawienia hasła roota oraz dodania użytkownika. Założone konto będzie podstawą codziennej pracy. Ważne jest, aby hasła dla obu kont nie były łatwe. Użytkownik będzie miał prawo zdalnego logowania, wiec proste słownikowe hasło może być zagrożeniem dla bezpieczeństwa serwera (*Rysunek 5: Hasło konta root i zakładanie użytkownika*).

Rysunek 5: Hasło konta root i zakładanie użytkownika

Następnie należy się zalogować na właśnie utworzone konto użytkownika (*Rysunek 6: Okno logowania do systemu*).



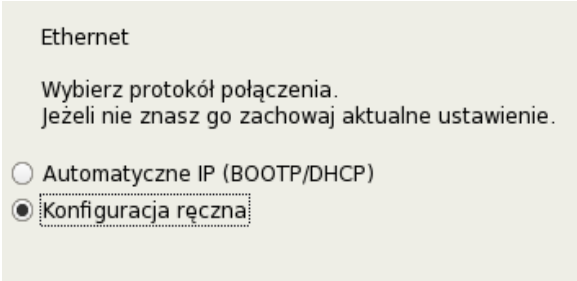
Rysunek 6: Okno logowania do systemu

Teraz w pierwszej kolejności trzeba przeprowadzić konfigurację sieci (*Rysunek 7: Ikona Konfiguracji połączenia*). Jeśli nasz serwer będzie podłączony bezpośrednio do łącza typu DSL ze stałym numerem IP, trzeba przygotować sobie dane od dostawcy internetu. Serwer powinien mieć stały IP na karcie WAN, dlatego najlepiej skonfigurować odpowiednio router nadrzędny, aby zarezerwować określony IP dla serwera podając MAC karty WAN.

Najistotniejsza jest identyfikacja kart sieciowych. Dobrze wiedzieć, jakie karty zainstalowane są w komputerze. Identyfikacja jest łatwiejsza, jeśli mamy dwie różne karty, zaś jeśli są dwie identyczne – system pokaże nam je w odwrotnej kolejności. Łączem WAN powinna być karta sieciowa eth0.

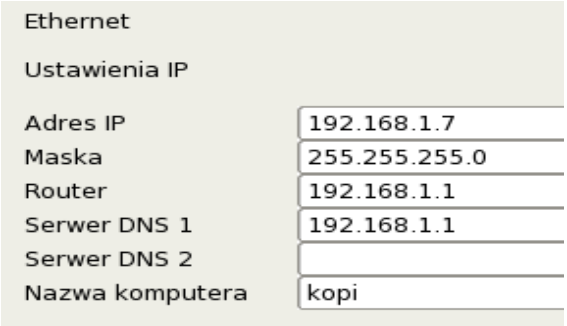
Aby skonfigurować sieć, trzeba uruchomić *Konfigurację Komputera*, ikonka programu znajduje się w pasku szybkiego uruchamiania. Jeśli naprawdę nie wiemy, która karta jest kartą eth0, można to sprawdzić klikając ikonę „*Konfiguracja interfejsu...*" (Zobacz w rozdziale dotyczącym konfiguracji ADSL. *Rysunek 11: Identyfikacja kart sieciowych*).

Rysunek 7: Ikona Konfiguracji połączenia



Rysunek 8: Ręczna konfiguracja karty Ethernet

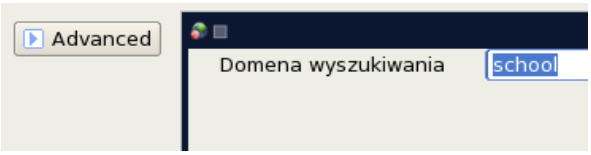
W zakładce *Internet i sieć* jest opcja konfigurowania nowego połączenia. Wybieramy konfigurację ręczną (*Rysunek 8: Ręczna konfiguracja karty Ethernet*) i podajemy IP, maska i brama wpiszą się automatycznie – trzeba jednak sprawdzić, czy będą to wpisy zgodne z danymi naszej sieci. Przydatne będą szczególnie dane dostawcy internetu, które znaleźć można w umowie (*Rysunek 9: Ręczne ustawienia numeru IP, maski oraz dns*).
Jeśli podłączymy serwer do routera sprzętowego, też dobrze mieć pewność, że wszystkie dane są prawidłowe, inaczej dostępu do internetu nie będzie.



Rysunek 9: Ręczne ustawienia numeru IP, maski oraz dns

Podajemy przynajmniej jeden nadrzędny serwer nazw (*DNS*) i wpisujemy nazwę komputera kopi. Domyślne serwery nazw TP S.A. to *194.204.159.1* i *194.204.152.34*.

Na koniec zaznaczamy opcję uruchamiania przy starcie i kończymy konfigurację.
W drugiej kolejności konfigurujemy kartę LAN czyli eth1. Robimy to identycznie, z tym, że adres IP wpisujemy *192.168.100.1* maskę *255.255.255.0* **a pozostałe pola mają zostać puste**. Oczywiście można zdefiniować inny numer IP, ale trzeba pamiętać, że wtedy ręcznie musimy ponownie konfigurować *dhcp*, *sambę*, *squida*, a także zmienić zawartość pliku */etc/hosts* (również na stacjach roboczych). Jedyną różnicą w konfiguracji sieci LAN



Rysunek 10: Domena wyszukiwania lokalnego

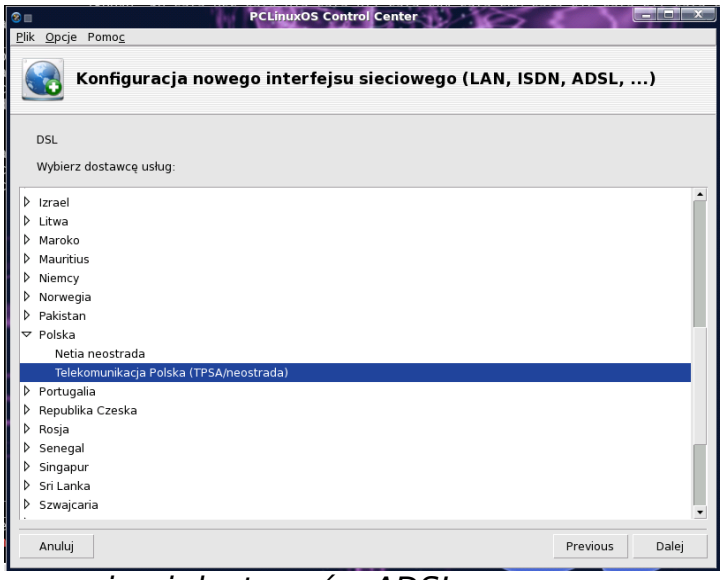
jest to, że klikamy przycisk *Advanced* i wpisujemy domenę wyszukiwania. Jest to potrzebne, jeśli zamierzamy korzystać z samby (*Rysunek 10: Domena wyszukiwania lokalnego*).

Konfiguracja ADSL

Domyślnie **EOS** przeznaczony jest i wstępnie skonfigurowany do pracy na łączach *DSL*, jednak skonfigurowanie połączenia z Neostradą jest banalnie proste. Najpierw w *Centrum konfiguracji sieci* należy sprawdzić, która z kart jest identyfikowana jako *eth1*. Gdy pojawi się pytanie o kartę sieciową do połączenia PPP, wskażemy właśnie tę (*Rysunek 11: Identyfikacja kart sieciowych*).

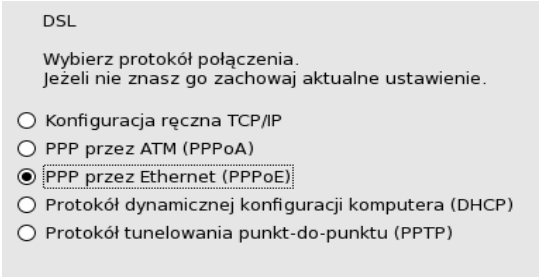
Rysunek 11: Identyfikacja kart sieciowych

Następnie wybieramy konfigurację nowego połączenia i wybieramy opcję DSL.W kolejnym oknie otworzą nam się dwie opcje dotyczące Polski – *Netia* i *Telekomunikacja Polska*. Dla *Neostrady* wybieramy drugą i przechodzimy do następnego okna (*Rysunek 12: okno z opcjami dostawców ADSL*).



Rysunek 12: okno z opcjami dostawców ADSL

Ponieważ mamy modem z gniazdem *RJ45* (np. *Speedtouch 510*), wybieramy opcję *PPPoE* (*Rysunek 13: Konfiguracja PPPOE dla Neostrady*).

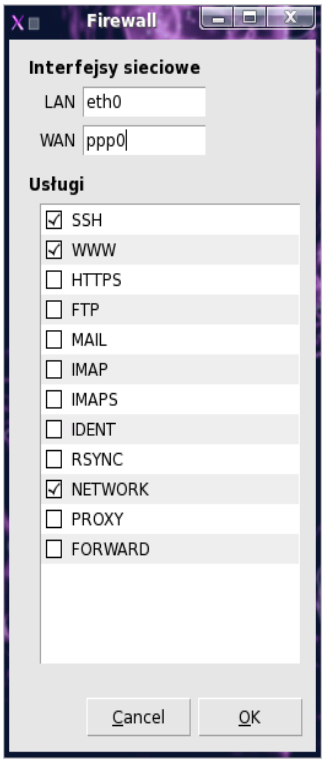


Rysunek 13: Konfiguracja PPPOE dla Neostrady

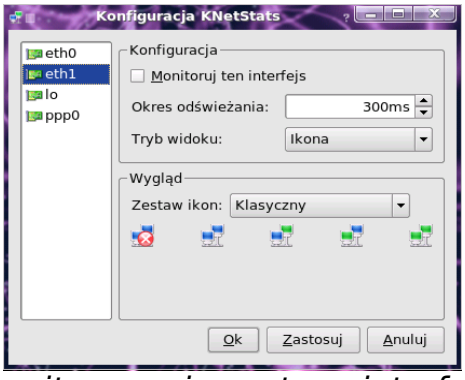
Teraz trzeba będzie wpisać swój login użytkownika i hasło do Neostrady, a

następnie zaznaczyć opcję „*Uruchom przy starcie systemu*”. Odpowiadamy jeszcze twierdząco na pytanie, czy chcemy zacząć w tej chwili i po kilkunastu sekundach połączenie się rozpocznie. Połączenie będzie zestawiane po każdym starcie systemu. Po skonfigurowaniu połączenia, niezbędne jest skonfigurowanie i ponowne uruchomienie firewalla (*Rysunek 14: Okno konfiguracji Firewalla*). Jako interfejs *WAN* podajemy *ppp0*, a LAN *eth0*. Interfejs *eth1* podłączony do modemu Neostrady będzie używany wyłącznie fizycznie. Aby w tacce systemowej nie pokazywał nam się niepotrzebnie należy skonfigurować aplet sieciowy. Trzeba prawym klawiszem myszy kliknąć na ikonce interfejsu i odznaczyć w okienku konfiguracji niepotrzebny interfejs(*Rysunek 15: Usunięcie monitorowania pustego interfejsu*).

Dalsza konfiguracja usług i ich uruchamianie jest już identyczne jak przy połączeniach DSL. Pamiętać należy jednak, że przy dynamicznym IP Neostrady, niektóre usługi związane z adresem serwera mogą nie pracować poprawnie po zmianie, która następuje co 24 godziny. Do takich usług należy program do dynamicznego dzielenia łącza – niceshaper. Standardowo wpisy uruchamiające program znajdują się w pliku *rc.local*, dla łącz ADSL lepiej przenieść te wpisy do */etc/ppp/if-up*.



Rysunek 14: Okno konfiguracji Firewalla



Rysunek 15: Usunięcie monitorowania pustego interfejsu

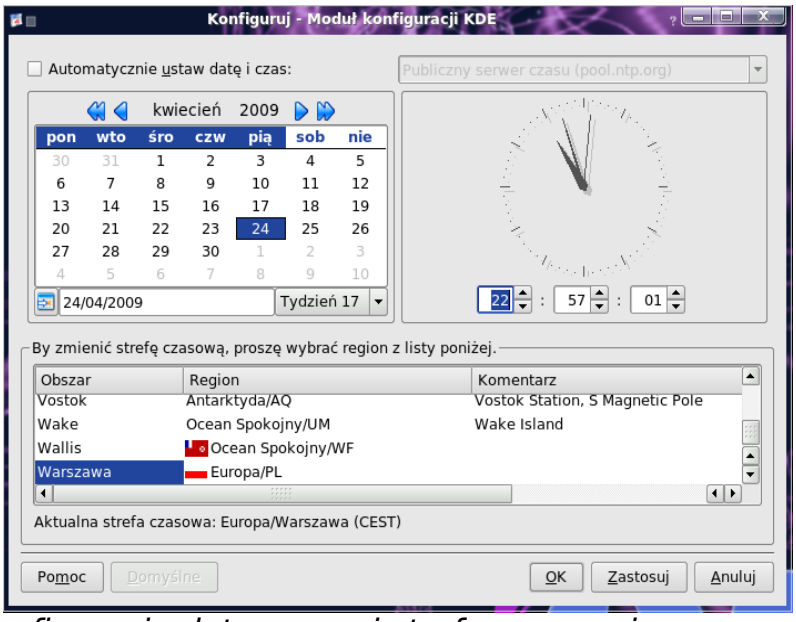
Inne typy połączeń sieciowych

Nie jest wskazane ustawianie interfejsu WAN jako dynamicznego połączenia z IP otrzymywanym przez *DHCP*. Jednak jest to możliwe i w większości przypadków będzie działać poprawnie. Lepiej jednak zadbać aby router nadrzędny przydzielał zawsze ten sam numer IP. Jeśli jest taka konieczność, interfejsem WAN może być karta sieciowa *eth1* (np. z powodu rejestracji adresu MAC u dostawcy). Jeśli interfejsem WAN jest karta radiowa, będzie ona identyfikowana często jako np. *wlan0*, *wifi0*, *ath0* lub *ra0* w zależności od stosowanego sterownika. Należy pamiętać przy niestandardowej konfiguracji o zmianach w firewallu, w przeciwnym razie system nie będzie działać poprawnie.

Konfiguracja komputera i usług

Zegar i strefa czasowa

Jedną z pierwszych czynności po instalacji systemu powinno być ustawienie czasu i strefy czasowej, w tym celu należy kliknąć prawym klawiszem myszy na zegarze w tacce systemowej i wybrać opcje „*Ustawienie daty i czasu*”.
W oknie konfiguracji (*Rysunek 16: Konfiguracja daty, czasu i strefy czasowej*) sprawdzamy, czy wybraną strefa jest Warszawa. Jeśli nie to zmieniamy strefę i klikamy „*Zastosuj*”. Następnie dokładnie ustawiamy czas i klikamy „*OK*”.



Rysunek 16: Konfiguracja daty, czasu i strefy czasowej

Konfiguracja filtrowania treści

Dansguardian i Squid

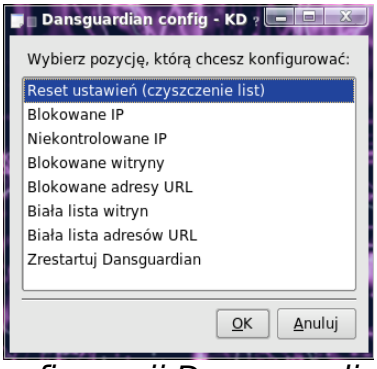
Dansguardian jest programem służącym do filtrowania treści na komputerach w sieci *LAN*. Działa na podstawie zestawu reguł wpisanych w plikach konfiguracyjnych, kontrolując ściągane strony w oparciu o heurystyczną analizę zawartości. Dodatkowo

pozwala na definiowanie własnych reguł użytkownika, co dodatkowo zabezpiecza sieć przed niepożądanymi stronami. Dansguardian współpracuje z lokalnym serwerem proxy – Squid. Ponieważ szkoły mają obowiązek stosowania oprogramowania filtrującego, jest to najlepszy wybór – wysoka skuteczność i dobra konfigurowalność za cenę niewielkiego wysiłku administratora – program jest darmowy.

Konfiguracja

Oprócz zestawu reguł wbudowanych, użytkownik ma możliwość decydowania o dodatkowych regułach filtrowania. Konfigurator umożliwia kontrolę sześciu aspektów działania programu.

Po uruchomieniu kreatora zobaczymy opcje możliwe do konfigurowania. W



Rysunek 17: Główne okno konfiguracji Dansguardiana

przypadku zbyt wielu niepotrzebnych lub wadliwych wpisów można skorzystać z opcji *Reset ustawień*. (*Rysunek 17: Główne okno konfiguracji Dansguardiana*).

Pierwszą opcją jest blokowanie numerów IP we własnej sieci lokalnej. Komputer wpisany na taka listę, nie będzie miał dostępu do internetu. Można również jednym wpisem zablokować całą sieć. Wówczas zamiast pojedynczego IP należy wpisać adres sieci z maską, np. 192.168.100.0/24. Opcja druga to wyłączenie poszczególnych komputerów spod kontroli *Dansguardiana*, może to być przydatne w sieci szkolnej do wpisania np. numeru IP komputera nauczycielskiego. Można również sobie wyobrazić sytuacje inną – w sieci abonenckiej domyślnie wyłączamy wszystkie komputery z ochrony i usuwamy z tej listy te, których użytkownicy wyraźnie życzą sobie ochrony np. ze względu na korzystające z komputera dzieci.

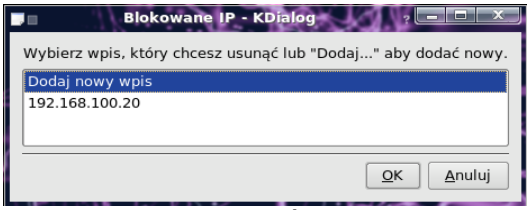
Kolejna z opcji dotyczy blokowania całych domen. Tu ważny jest sposób wpisania domeny. Gdy wpiszemy *wp.pl*, to zablokowane zostaną wszystkie strony w tej domenie, a więc także i te, których wcale blokować nie chcemy, np. *tv.wp.pl*. Z tego względu nie należy blokować domeny głównej, a najczęściej subdomenę, np. *erotyka.wp.pl*.

Opcja następna to blokowanie adresów URL. Czasem zdarza się, że w jakiejś domenie znajduje się strona, której wyświetlać nie chcemy, a nie jest ona oznaczona subdomeną. Niewłaściwa strona znajduje się np. pod adresem *http://dobra.strona.pl/porno*. Wówczas dodajemy ją do zablokowanych adresów URL w postaci *dobra.strona.pl/porno* (bez *http://*).

Można też dodać określone domeny do własnej białej listy. Problem z blokowaniem zwykle dotyka portali. Czasem na stronie portalu mogą sie zdarzyć informacje i odnośniki odczytane przez program w ten sposób, że przekroczą tzw. limit wagowy fraz i portal zostanie zablokowany. Aby tego uniknąć możemy dodać portal do białej listy np. *wiadomości.gazeta.pl*.

Na podobnej zasadzie możemy używać białej listy URL. Tutaj najczęściej problem dotyczy darmowych kont hostingowych. Dla przykładu w domenie hosting.pl większość stron powinna być blokowana, ale znajduje się tam strona, do której chcemy mieć dostęp. Strona znajduje się pod adresem *http://hosting.pl/dobrastrona* i wówczas dodajemy ją do

białej listy URL wpisem *hosting.pl/dobrastrona* (bez *http://*). Wybranie każdej opcji konfiguracyjnej w pierwszym okienku spowoduje pojawienie się następnego okna.



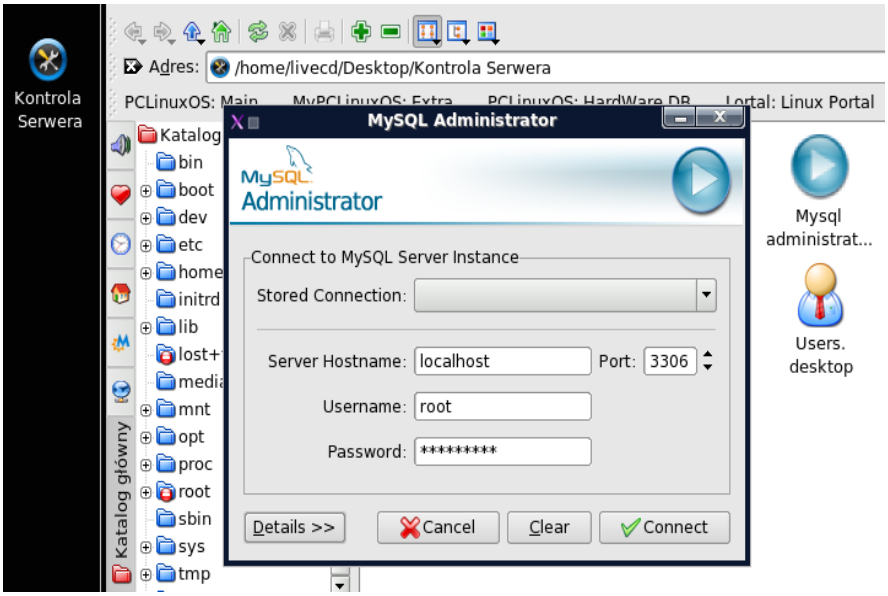
Rysunek 18: Dodawanie i usuwanie wpisów konfiguracyjnych

Możemy dodać wpis, lub usunąć któryś z istniejących. Kliknięcie przycisku ”Anuluj” spowoduje powrót do głównego okna skryptu(*Rysunek 18: Dodawanie i usuwanie wpisów konfiguracyjnych*). Po w prowadzeniu zmian, należy wybrać opcję restartu programu, aby zmiany zaczęły obowiązywać.

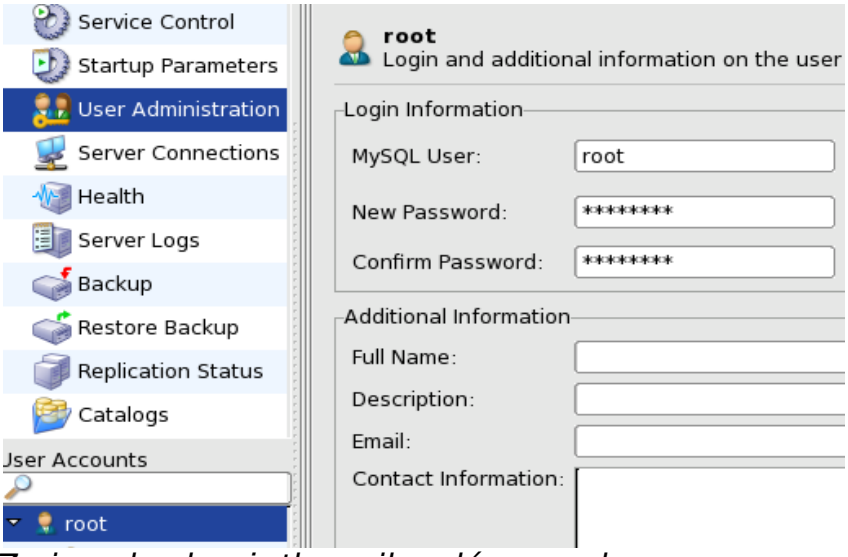
Zarządzanie MySQL

Zmiana domyślnego hasła

Pierwszą czynnością po zainstalowaniu nowego serwera powinna być zmiana wszystkich domyślnych haseł, w tym hasła do bazy *MySQL*. Należy upewnić się, że usługa *MySQL* działa i następnie wybrać z menu program zarządzający *Mysql Administrator*. Zalogować się z domyślnym hasłem i następnie przejść do zakładki *User Administration*, niżej zaznaczyć użytkownika root i wpisać nowe hasło dwukrotnie (Rysunek 19: Logowanie do programy MySQL Administrator *i Rysunek 20: Zmiana hasła użytkownika głównego bazy*). Na koniec klikamy przycisk *Change* i zamykamy program. W identyczny sposób można zmienić hasła użytkowników z dostępem do bazy *Moodle*, poczta i *Roundcubemail*, jednak należy pamiętać, aby potem zmienić również hasła w plikach konfiguracyjnych, w przeciwnym razie usługi zależne od tych baz nie będą działać z powodu braku dostępu do bazy. Domyślne hasła do wszystkich baz znajdują się w pliku, który otwiera się automatycznie po pierwszym zalogowaniu do systemu.

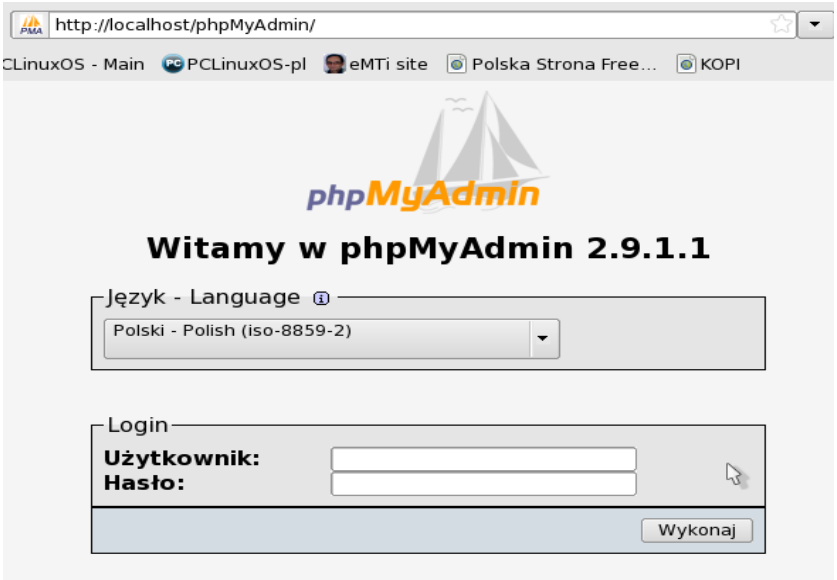


Rysunek 19: Logowanie do programy MySQL Administrator



Rysunek 20: Zmiana hasła użytkownika głównego bazy

W dalszym zarządzaniu bazą *MySQL* możemy korzystać z tego programu, lecz łatwiej będzie korzystać z webowego interfejsu *phpMyAdmin*. Wywołujemy go, w przeglądarce wpisując w pasku adresu *http://localhost/phpMyAdmin*. Za pomocą interfejsu webowego można w łatwy sposób zarządzać istniejącymi bazami i dodawać nowe. Czytelna struktura interfejsu pozwala na modyfikacje tabel i pojedynczych rekordów, ale także na wydawanie standardowych poleceń *MySQL* (*Rysunek 21: Okno logowania phpMyAdmin*). Strona phpMyAdmin dostępna jest wyłącznie z serwera. Można ją odblokować edytując plik */etc/httpd/conf/webapps.d/phpMyAdmin.conf*. Należy dla katalogu *phpMyAdmin* ustawić wówczas opcję *Allow from All*. na koniec trzeba zrestartować usługę *httpd*.

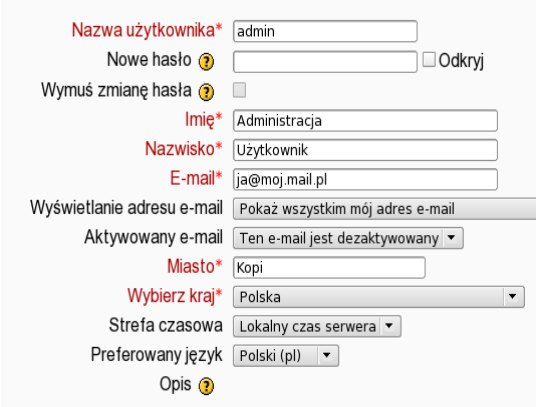


Rysunek 21: Okno logowania phpMyAdmin

Zarządzanie serwerem www i Moodle

Serwer *Apache* działa bez potrzeby konfiguracji. W przypadku posiadania domeny i chęci korzystania z subdomen, konieczna będzie ręczna edycja konfiguracji w */etc/httpd*. Jest to jednak zadanie dla zaawansowanych użytkowników. Jednak hasło administratora

Moodle powinien zmienić każdy. W przeglądarce wpisujemy w pasku adresu: *http://localhost/moodle* i klikamy link „*Zaloguj*” w prawym górnym rogu. Potem należy kliknąć link „*Użytkownik*”, i przejść do zakładki „*Modyfikuj profil*”.



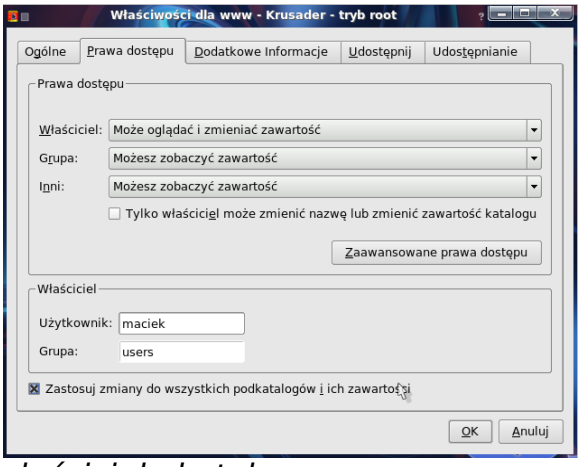
Rysunek 22: Okno ustawień panelu Moodle

Należy tam wpisać nowe hasło, ale także swój prawdziwy e-mail, który będzie potrzebny do zarządzania i pracy, a również inne elementy profilu (*Rysunek 22: Okno ustawień panelu Moodle*).

Aby strona poprawnie wyświetlała się nie tylko w wewnętrznej sieci, należy zmienić wpis: *$CFG->wwwroot = „http://192.168.100.1/moodle”;* w pliku konfiguracyjnym na domenę własną, w której pracuje serwer np. *http://szkola.domena.pl/moodle*.

Platforma zdalnego nauczania Moodle jest efektywnym i nowoczesnym systemem, ale podobnie jak inne programy wymaga zapoznania się z nim. Rolą administratora będzie dodanie nowych użytkowników z uprawnieniami nauczycieli, którzy będą mogli tworzyć nowe kursy oraz zarządzać nimi. Szczegółowe porady, można znaleźć na wielu stronach internetowych.

Katalogiem stron jest */var/www/html* i w nim znajduje się też domyślna strona, którą można przystosować do własnych potrzeb. Na stronie wyświetla się krótka instrukcja. Jeśli jednak użytkownik będzie chciał umieścić własną stronę, najlepiej jeśli zmieni właściciela katalogu */var/www*, którym jest root. Można to najprościej wykonać poleceniem konsolowym z konta roota: *chown -R nazwa_konta.users /var/www*. Można też uruchomić program *Krusader* w trybie administratora i prawym klawiszem kliknąć na katalogu, a potem wybrać *Właściwości*. W zakładce Prawa dostępu wpisać swoją nazwę użytkownika i grupę users oraz zaznaczyć opcję *Zastosuj zmiany do wszystkich podkatalogów i ich zawartości (Rysunek 23: Zmiana właściciela katalogu).* Teraz będzie można edytować pliki nie używając konta roota.



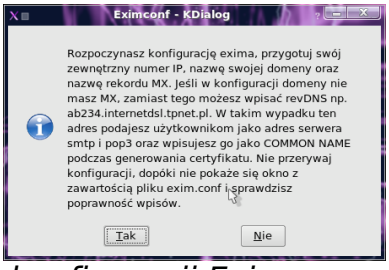
Rysunek 23: Zmiana właściciela katalogu

Konfiguracja poczty

Konfiguracja Exima

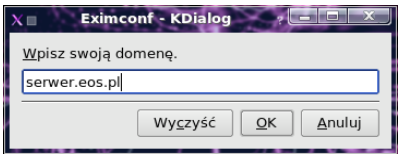
Aby skonfigurować serwery poczty elektronicznej (SMTP i POP3), trzeba zarejestrować domenę i nie należy tego mylić z czymś co nazywane jest domeną na serwerach SBS. Ponieważ konfiguracja w systemie eos zakłada konfigurację poczty z użytkownikami wirtualnymi, należy wymyślić nazwę konta, które będzie dostawać pocztę roota.

Należy uruchomić konfigurator serwera SMTP (*Rysunek 24: Okno startowe konfiguracji Exima*), należy podać hasło roota i przeczytać informację, kliknąć *Tak*, jeżeli chcemy przeprowadzić konfigurację.



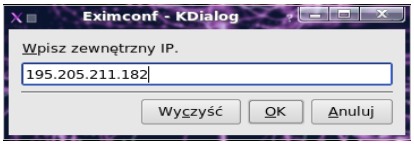
Rysunek 24: Okno startowe konfiguracji Exima

Konfiguracja wymaga podania trzech wartości z naszej konfiguracji sieciowej i konfiguracji domeny. Potrzebna będzie nazwa domeny np. *serwer.eos.pl*, prawidłowo powinniśmy w konfiguracji strefy podać rekord *MX*, przydaje się on szczególnie, gdy mamy w tej samej domenie kilka serwerów z różnymi IP. Niektóre serwery poczty mogą nawet odrzucać pocztę z serwera bez rekordu *MX*, zatem lepiej to stosować. Nazwa *MX* różni się od podstawowej domeny z reguły przedrostkiem np. *mail.serwer.eos.pl* (czasem może być taka sama jak domena). Jeśli nie mamy możliwości skonfigurować rekordu MX należy wykorzystać *revDNS* naszego numeru IP (na hoście bez *revDNS* w ogóle nie warto zakładać serwera poczty). Ze względu na problem spamu, coraz więcej serwerów nakłada ostre restrykcje i sprawdza konfigurację nadawców. Warto *revDNS* mieć taki sam jak rekord *MX* (oczywiście jeśli mamy na to wpływ). W przypadku wykorzystania revDNS zamiast *MX*, najlepiej będzie jeśli w ustawieniach użytkowników ten adres będzie właśnie adresem serwera *SMTP* i *POP3*.
Pierwsze okno konfiguracji zapyta o nazwę domeny (*Rysunek 25: Wpisanie domeny serwera*).



Rysunek 25: Wpisanie domeny serwera

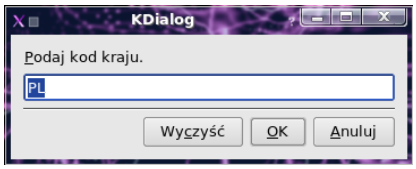
Następnie pojawi się pytanie o rekord *MX*. Ostatnie z okienek zapyta o zewnętrzny numer IP. W tym wypadku najlepiej mieć serwer włączony bezpośrednio do internetu, jednak jeśli nawet podłączamy serwer za pośrednictwem maskującego IP routera (ze skonfigurowaną strefą *DMZ* dla naszego serwera lub forwardem portów), to zawsze podajemy IP pod jakim będzie nasz serwer widziany z internetu (*Rysunek 26: Ostatnie pytanie dotyczy zewnętrznego numeru IP serwera*).



Rysunek 26: Ostatnie pytanie dotyczy zewnętrznego numeru IP serwera

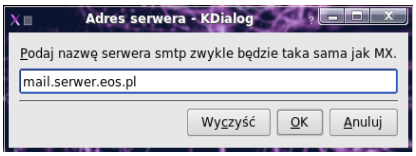
Gdy zakończymy ten etap, pojawi się okno z zawartością pliku exim.conf, w którym można sprawdzić, czy nie zaszła żadna pomyłka. Zamykamy to okno i możemy przejść do konfiguracji certyfikatów. Na samym końcu wpiszemy jeszcze nazwę konta, które będzie otrzymywać pocztę roota (np. nauczyciel@moja.domena.pl).

Po uruchomieniu generatora certyfikatów, pojawi się najpierw okno z ostrzeżeniem, że dane certyfikatu nie mogą być wymyślone. Certyfikat nie będzie uwierzytelniony przez żadne centrum certyfikacji (jest to zbyt drogie), więc należy być pewnym , że użytkownik sprawdzający certyfikat na swoim komputerze, zamiast poprawnej nazwy i adresu nie zobaczy jakiegoś bełkotu.



Rysunek 27: Najpierw należy podać dwuliterowy kod kraju

Należy podać prawidłowo dwuliterowy kod kraju (*Rysunek 27: Najpierw należy podać dwuliterowy kod kraju*), nazwę województwa, miejscowości i najważniejsze adres serwera – ma to być ten sam adres z którym będzie sie łączył użytkownik odbierając lub wysyłając pocztę (*Rysunek 28: Adres serwera do certyfikatu*). Nie zawsze będzie taki sam jak drugi człon w adresie e-mail. Posługując się wcześniejszym przykładem konfiguracji – będzie to adres mail.serwer.eos.pl.



Rysunek 28: Adres serwera do certyfikatu

Dobrym zwyczajem jest podawanie czynnego maila administratora domeny, a nie adresu wymyślonego na poczekaniu. Na koniec zobaczymy okienko z komunikatem o przeprowadzeniu konfiguracji. Teraz wystarczy w oknie zarządzania usługami włączyć usługi: clamd, exim, imapd (dla webmaila) i tpop3d (okno panelu z uruchamianiem usług – *Rysunek 82: Okno zarządzania usługami w panelu administracyjnym*). Oczywiście trzeba zaznaczyć przy nich opcję „On boot”, żeby się uruchamiały automatycznie po starcie systemu. Uwaga, przeprowadzenie konfiguracji serwera, czy wygenerowanie certyfikatu powoduje, że poprzednie dane są kasowane, więc warto się zastanowić, zanim kliknie się *Tak*.

Administracja użytkownikami

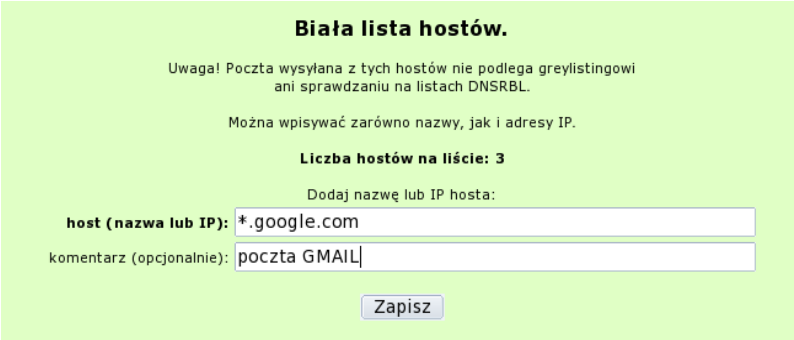
Serwer poczty jest skonfigurowany do stosowania kont wirtualnych, a nie systemowych. Zarządzanie kontami jest łatwe dzięki panelowi administracyjnemu. W pasku adresu przeglądarki należy wpisać *http://localhost/mailadmin* (lub adres serwera) i najpierw wygenerować hasło użytkownika admin. Po chwili pojawi się strona logowania, po wpisaniu loginu i hasła pierwszą czynnością powinno być dodanie naszej domeny (*Rysunek 29: Dodawanie domeny w panelu Mailadmin*).

Rysunek 29: Dodawanie domeny w panelu Mailadmin

Tym razem nie podajemy adresu serwera smtp tylko nazwę domeny, w której będą swoją pocztę mieli użytkownicy (z adresami typu *nazwa@serwer.eos.pl*). W następnej kolejności dodajemy użytkowników, możemy też im włączyć korzystanie z *FTP*. Jako pierwsze dodajemy konto, które wcześniej zdefiniowaliśmy jako to, **które będzie dostawać pocztę roota**. To powinno być konto, które należy regularnie sprawdzać, bowiem się pojawią na nim rozmaity komunikaty systemowe, ale też np. informacje od innych serwerów, które mogą nas ostrzec, że coś w sieci się dzieje, co niekoniecznie się nam spodoba. Serwer SMTP domyślnie korzysta z tzw. greylistingu, który bardzo skutecznie chroni przed zalewem spamu z rozmaitych botów. Greylisting może być korygowany przez dodawanie do własnej białej listy hostów lub nadawców, którzy zasługują na zaufanie(*Rysunek 30: Menu białych list w panelu pocztowym)*. Należy przy tym pamiętać, że najbardziej bezpieczne jest dodawanie hostów (czyli IP, MX lub revDNS odległego serwera poczty), ponieważ adres mailowy nadawcy można sfałszować. Tylko w wyjątkowych przypadkach należy korzystać z ostatniej opcji – białej listy adresatów, ponieważ te konta nie będą wówczas chronione przed spamem.

Rysunek 30: Menu białych list w panelu pocztowym

W przypadku dużych serwerów, korzystających z wielu numerów IP greylisting może znacząco opóźniać dostarczenie poczty. Dlatego warto dodawać je do własnej białej listy w postaci takiej jak na rysunku (*Rysunek 31: Dodanie poczty GMAIL do białej listy*).



Rysunek 31: Dodanie poczty GMAIL do białej listy

Oprócz białych list, administrator ma także do dyspozycji czarne listy. Można wpisywać hosty lub nadawców, w tym także nazwy cząstkowe uzupełnione znakiem * zamiast dowolnego ciągu. W ten sposób można zablokować szczególnie uciążliwe hosty lub nadawców. Należy to jednak robić ostrożnie i z namysłem. Wpisanie bowiem np *zosia@** do czarnej listy spowoduje, że nigdy nie zostanie wpuszczona poczta od użytkownika *zosia*, obojętnie z jakiego serwera.

Użytkownicy mają do dyspozycji Webmail, który posiada panel zmiany hasła użytkowników. Jest to istotne, bowiem nieistniejące w systemie konta innej możliwości nie mają. Panel pocztowy (*Rysunek 32: Panel logowania - Webmail*) dla użytkowników jest dostępny pod adresem *http://adres.serwera/poczta*.

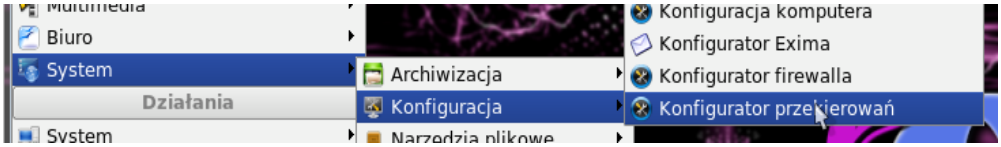
Rysunek 32: Panel logowania - Webmail

Dodatkowe usługi – imapd (do odbioru poczty przez webmaila) oraz tpop3d (serwer POP3) nie wymagają dodatkowej konfiguracji. Podsumowując, konfiguracja poczty jest w systemie **Eos** bardzo prosta, ale jeśli nie wiesz, co to jest domena, rekord MX, revDNS, nie potrafisz zidentyfikować zewnętrznego IP serwera, to najprawdopodobniej nie powinieneś być administratorem własnej poczty.

Konfiguracja firewalla

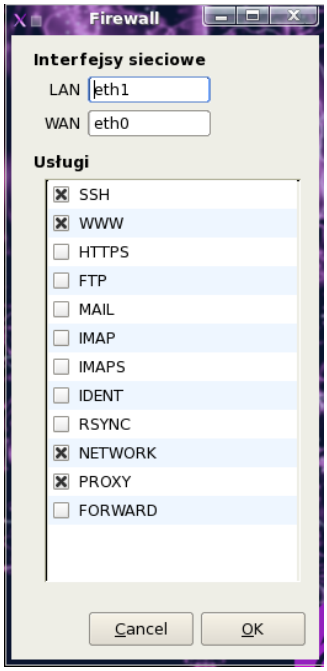
Podstawowe ustawienia

Firewall jest zestawem reguł wykonywanych przez iptables, które zapewniają bezpieczeństwo serwerowi i sieci lokalnej. Jego zadaniem jest filtrowanie ruchu na interfejsie zewnętrznym, maskowanie komputerów w sieci lokalnej oraz forwardowanie pakietów. Jest także możliwe przekierowanie określonych portów na dowolny komputer w sieci. Konfigurator firewalla uruchamiamy z menu *System* w grupie programów *Konfiguracja*(*Rysunek 33: Menu systemowe - Konfiguracja*).



Rysunek 33: Menu systemowe - Konfiguracja

Po podaniu hasła roota zobaczymy okno konfiguratora z domyślnymi ustawieniami



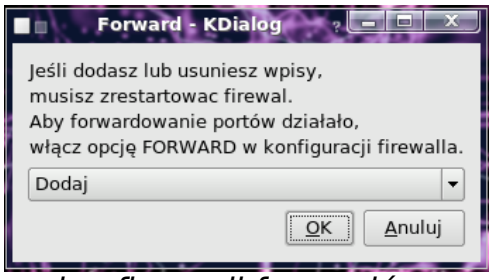
Rysunek 34: Konfiguracja Firewalla

(*Rysunek 34: Konfiguracja Firewalla*). Jako pierwsze podane są interfejsy sieciowe, jeśli nasza konfiguracja sieciowa różni się, np. interfejs WAN to *ppp0*, należy to zmienić w konfiguratorze (*patrz: konfiguracja neostrady*). Kolejne wpisy dotyczą usług działających na serwerze. Domyślnie włączone jest SSH, ponieważ zapewnia możliwość zdalnej administracji. Włączony jest także dostęp do serwera www. Pozostałe usługi można udostępnić, jeśli zostaną skonfigurowane i włączone.

Kolejny ważny wpis to *NETWORK*, oznacza on, że komputer udostępnia internet stacjom w sieci wewnętrznej, jeśli ta opcja zostanie odznaczona, komputery nie będą miały dostępu do internetu. Następna jest pozycja *PROXY*, powoduje ona, że korzystanie z internetu na stacjach klienckich odbywa się przez tzw. pośrednika, czyli serwer proxy z filtrowaniem treści. Odbywa się to w sposób przezroczysty, czyli niezależny od ustawień użytkownika. Jeśli tę opcję wyłączymy, komputery klienckie nie będą chronione przed niepożądaną zawartością. Ważna opcja, to *FORWARD*. Włączenie jej umożliwia skonfigurowanie przekierowania portu z interfejsu zewnętrznego na port w dowolnym komputerze sieci wewnętrznej. Opcja *NICESHAPER* decyduje w włączeniu lub wyłączeniu dynamicznego dzielenia łącza. Po zmianie ustawień należy kliknąć *OK*, żeby zapisać ustawienia i zamknąć konfigurator.

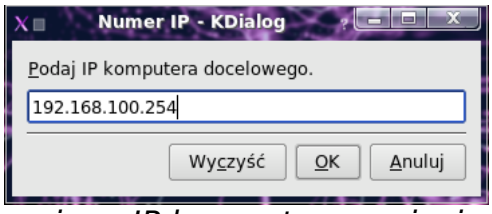
Przekierowanie portów

Dodatkowy konfigurator (Rysunek 35: Pierwsze okno konfiguracji forwardów) przekierowań portów będzie przydatny, jeśli trzeba przekierować port z sieci wewnętrznej tak, aby był widoczny z internetu. Przykładowo, może to być urządzenie dostępu radiowego (access point), którym można zarządzać przez przeglądarkę.



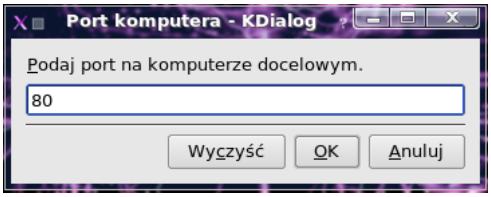
Rysunek 35: Pierwsze okno konfiguracji forwardów

Użytkownik może usunąć istniejące reguły lub dodawać nowe. Opcja *Dodaj* wymaga podania trzech wartości. Najpierw należy podać numer IP urządzenia w sieci wewnętrznej(*Rysunek 36: Dodawanie wpisu - IP komputera w sieci*).



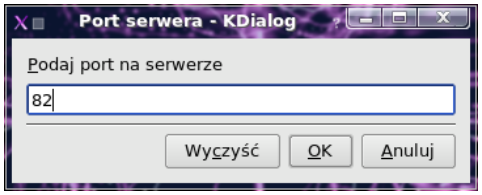
Rysunek 36: Dodawanie wpisu - IP komputera w sieci

Następnie trzeba podać port (*Rysunek 37: Dodawanie wpisu - port usługi*) pracującej na tym urządzeniu usługi, w naszym przykładzie będzie to port 80 (zarządzanie AP przez www).



Rysunek 37: Dodawanie wpisu - port usługi

Teraz trzeba wybrać port który będzie otwarty na serwerze. W naszym przypadku nie może być to port 80, bo na nim już pracuje serwer www. Nie można na ten sam port przekierować usług z dwóch różnych urządzeń. Zatem wybierzemy port 82 i będąc w poza naszą siecią będziemy się łączyć z tym urządzeniem używając adresu *http://adres.serwera:82* (*Rysunek 38: Przekierowanie na inny port*), ale wewnątrz sieci to przekierowanie nie jest potrzebne, i w dalszym ciągu będziemy używać numeru IP urządzenia.



Rysunek 38: Przekierowanie na inny port

Dodanie lub usunięcie przekierowania wymagać będzie podania hasła roota przed zapisaniem nowych ustawień. Jeśli juz odpowiednie forwardy portów zostały dodane i, co ważne, opcja FORWARD w firewallu jest aktywna, aby wprowadzone zmiany odniosły skutek, trzeba zrestartować firewall. Należy otworzyć panel nazywający się *Konfiguracja komputera* i w zakładce *System* kliknąć *Zarządzanie usługami systemowymi*...

Rysunek 39: Restartowanie usługi w panelu Konfiguracja komputera

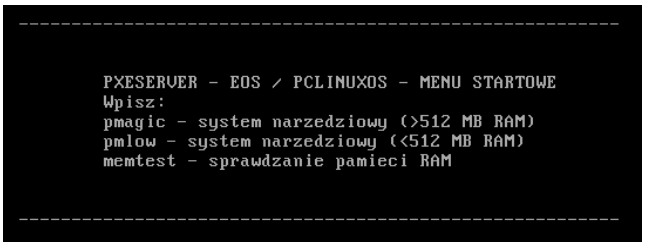
Trzeba kliknąć przycisk *Start* usługi *firewall*, który spowoduje ponowne uruchomienie usługi (*Rysunek 39: Restartowanie usługi w panelu Konfiguracja komputera*). Jako ciekawostkę podam, że ponowne uruchomienie usługi spowoduje też wpisanie w konsoli (jako root) polecenia *service firewall restart*.

System narzędziowy z PXE

Część komputerów, obecnie większość, ma możliwość startu i załadowania systemu operacyjnego bez instalowania go na dysku, a nawet bez ładowania go z dyskietki, czy płyty CD/DVD. Komputer startuje dzięki specjalnej karcie sieciowej, w której pamięci zapisanych jest kilka prostych procedur. Po starcie karta sieciowa pobiera adres z serwera *DHCP*, następnie z serwera za pośrednictwem *TFTP* pobierany jest plik rozruchowy, a następnie możliwe jest załadowanie systemu. Można w ten sposób uruchomić rozmaite systemy operacyjne. W Linuksie jest projekt *LTSP*, który można wykorzystać w pracowniach ze słabszymi komputerami – pod warunkiem posiadania odpowiednio mocnej maszyny na serwer.

EOS ma zaimplementowany serwer *PXE* z przydatnymi opcjami. Mogą się one przydać tam, gdzie w *LAN* są komputery zarządzane centralnie. Administrator może przy odrobinie chęci wykorzystać *PXE* do sieciowej instalacji *Linuksa*, a nawet *Windows* (jest linuksowa implementacja *RIS*). Jeśli jednak dysponujemy wersjami *OEM Windows*, to ich

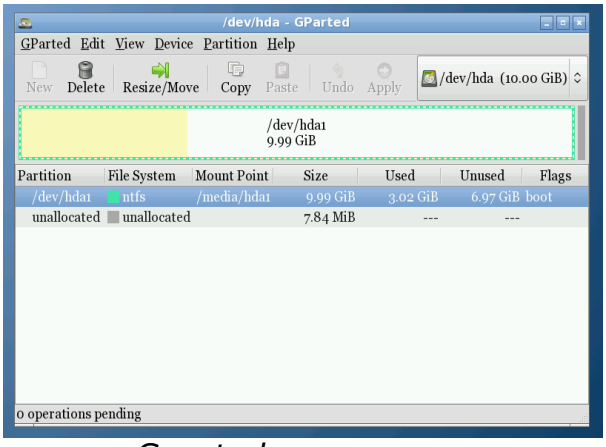
licencja nie zezwala na zdalną sieciową instalację nienadzorowaną. Jednak w pracowniach szkolnych sieciowa instalacja nienadzorowana jest możliwa i dozwolona. Licencjodawca nigdzie nie wykluczył stosowania innego systemu jako serwera instalacji. Po uruchomieniu komputera w sieci z *PXE* zobaczymy po chwili na ekranie menu (*Rysunek 40: Ekran startowy PXE w sieci z serwerem EOS*).



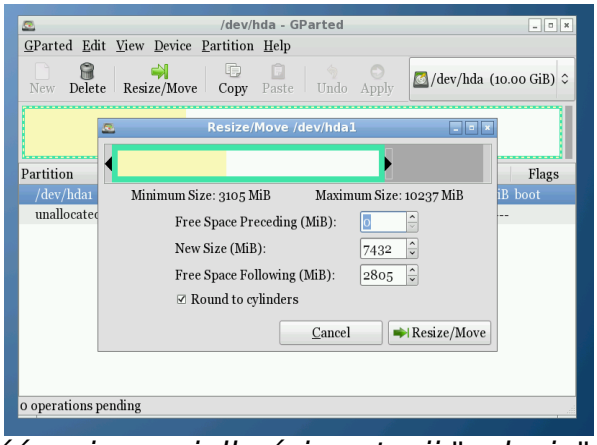
Rysunek 40: Ekran startowy PXE w sieci z serwerem EOS

Pierwsza opcja uruchamia okienkową dystrybucję narzędziową *Linuksa*, która zawiera podstawowe programy umożliwiające korzystanie z internetu, np. *Firefoxa*. Jednak nie to jest przeznaczeniem głównym dystrybucji *Pmagic*. Jest tam wiele przydatnych narzędzi, które np. potrafią nam zrobić kopie zapasowe partycji, zdiagnozować uszkodzenia dysku lub zmieniać wielkość partycji, czy zakładać nowe. Opcja druga to uruchomienie tego samego systemu, ale dla komputerów z mniejszą ilością pamięci. Orientacyjną granicą dla tych opcji jest 512 MB. Trzecia możliwość to uruchomienie programu *Memtest*. W razie problemów z komputerem, gdy system nie pracuje prawidłowo, warto użyć tej opcji, ponieważ często zdarza się, że to właśnie wady pamięci powodują problemy z systemem operacyjnym. System *Pmagic* może być przydatnym narzędziem administratora, więc warto się z nim zapoznać. Jednym z przydatnych narzędzi jest *Gparted*. Program ten umożliwia zakładanie i kasowanie partycji, a także zmianę ich wielkości bez utraty danych, choć należy pamiętać o wykonaniu kopii zapasowej ważnych danych.

Program pokazuje wielkość partycji oraz ilość zajętego na niej miejsca. Możemy zmniejszyć partycję NTFS, aby wygospodarować miejsce na Linuksa (Rysunek 41: Okno programu Gparted, *Rysunek 42: Możliwość zmiany wielkości partycji "w locie"*). Po podjęciu decyzji klikamy przycisk *Resize/Move*, a następnie *Apply* i program zaczyna pracę. Po zakończonej operacji możemy uruchomić Windows, a pozostałe wolne miejsce przeznaczyć do innych celów. W systemie *Pmagic* można znaleźć jeszcze wiele przydatnych programów zarówno do diagnozowania system, jak i do robienia obrazów partycji w celu wykonania kopii bezpieczeństwa, testowania dysku oraz naprawy systemu.



Rysunek 41: Okno programu Gparted



Rysunek 42: Możliwość zmiany wielkości partycji "w locie"

Dodatkowe możliwości daje system Clonezilla, który choć trudniejszy w użyciu, bo tekstowy, pozwala na wykonanie obrazu dysku komputera klienckiego na serwerze. Clonezilla ma wiele możliwości, w razie potrzeby możemy pracować bezpośrednio na urządzeniach, a więc klonować dyski, możemy wykonywać obrazy partycji i zapisywać je bezpośrednio na komputerze lub na zdalnym serwerze korzystając z połączenia *SSH* lub udostępnianych katalogów *Samby*, czy NFS. Najprostszym sposobem w sieci lokalnej z serwerem EOS jest skorzystanie z udostępnionych katalogów *NFS* w */home/nis*. Dla przykładu – obraz partycji o wielkości 8GB z wykorzystanym obszarem o wielkości 2,5 GB został zrobiony w ciągu dziesięciu minut i na serwerze zajmował ok 1,3 GB.

Zakładając, że administrator przygotuje modelowy system na stację, wraz ze wszystkimi programami i aktualizacjami, to można następnie taki system sklonować na pozostałe komputery w pracowni i jedyna czynność po zmianie nazwy maszyny to dodanie jej do domeny. Oczywiście ze względów licencyjnych nie wolno tego robić zbiorowo w przypadku licencji OEM.

```
Starting saving /dev/hda1 as /home/partimag/2009-05-12-23-img/hda1.XXX...
/dev/hda1 filesystem: ntfs.
*****************************************************.
Checking NTFS integrity in /dev/hda1... done!
Checking the disk space...
Use ntfsclone with gzip to save the image instead of partimage.
Image file will not be split.
*****************************************************.
If this action fails or hangs, check:
* Is the disk full ?
*****************************************************.
ntfsclone v2.0.0 (libntfs 10:0:0)
NTFS volume version: 3.1
Cluster size       : 4096 bytes
Current volume size: 10725732352 bytes (10726 MB)
Current device size: 10725732864 bytes (10726 MB)
Scanning volume ...
Total Time: 00:00:02, Ave. Rate:    0.0MB/min, 100.00% completed!
Accounting clusters ...
Space in use       : 2433 MB (22.7%)
Saving NTFS to image ...
Total Time: 00:10:46, Ave. Rate:  225.9MB/min, 100.00% completed!
Syncing ...
Checking the disk space...
>>> Time elapsed: 648.29 secs (~ 10.804 mins), average speed: 222.0 MB/min
*****************************************************.
Finished saving /dev/hda1 as /home/partimag/2009-05-12-23-img/hda1.ntfs-img
*****************************************************.
Saving hardware info by lshw...
Saving DMI info...
Saving package info...
*****************************************************.
*****************************************************
*****************************************************
This program is not started by Clonezilla server, so skip notifying it the job is done.
Finished!
Now syncing - flush filesystem buffers...
```

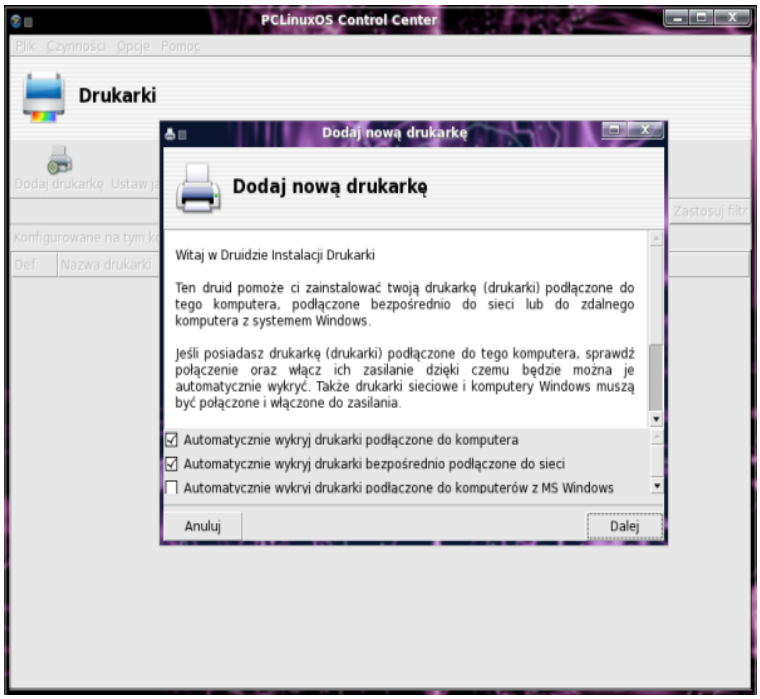
Rysunek 43: Wykonywanie kopii zapasowej partycji NTFS

Konfiguracja drukarki sieciowej

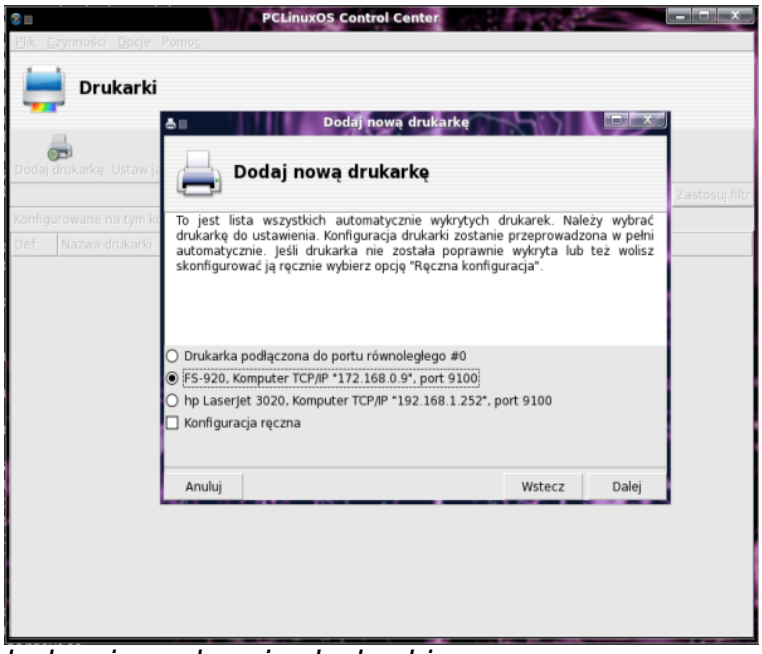
Obecnie używane drukarki mają najczęściej interfejs USB albo interfejs sieciowy (czasami jest to osobny niewielki printserver). W przypadku drukarek połączonych z komputerem kablem USB używamy serwera druku *Cups*, zarówno dodawanie drukarki jak i późniejsze użytkowanie jest identyczne, jak w przypadku drukarki sieciowej. Tańsze modele drukarek niektórych producentów wymagają pliku firmware przesyłanego z komputera do drukarki (dotyczy to wyłącznie modeli podłączanych do USB). Ze względów licencyjnych takie pliki trzeba pobrać samodzielnie.

Dla komputerów klienckich drukarka podłączona do serwera przez USB jest zwykłą drukarką sieciową i w przypadku stacji linuksowych nie wymaga instalowania sterowników. System Windows będzie natomiast potrzebował sterowników producenta sprzętu.

Instalację nowej drukarki rozpoczynamy w Konfiguracji komputera w zakładce sprzęt. Kreator potrafi sam wykryć zarówno drukarki podłączone lokalnie, podłączone do innych komputerów i sieciowo. Przed rozpoczęciem konfiguracji, należy się upewnić, że drukarka jest włączona i ma prawidłowy numer IP w sieci lokalnej. W przypadku, gdy zakres sieciowy w LAN się zmienia, należy użyć wcześniej panelu administracyjnego drukarki www (jeśli taki posiada), zmienić konfigurację bezpośrednio (w modelach z wyświetlaczem LCD) lub użyć do tego oprogramowania producenta. Dopiero po zmianie IP należy przystąpić do konfiguracji. Prawidłowo pracująca w sieci drukarka zostanie bez trudu wykryta i najczęściej prawidłowo zidentyfikowana. Baza obsługiwanego przez *Cups* sprzętu jest już bardzo duża i większość drukarek, które np. były dołączane do szkolnych pracowni będzie pracować bez trudu.



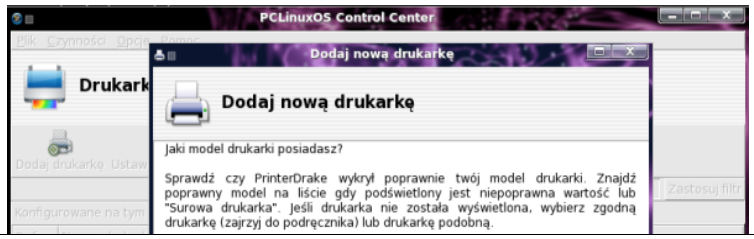
Rysunek 44: Krok pierwszy - dodaj nową drukarkę.

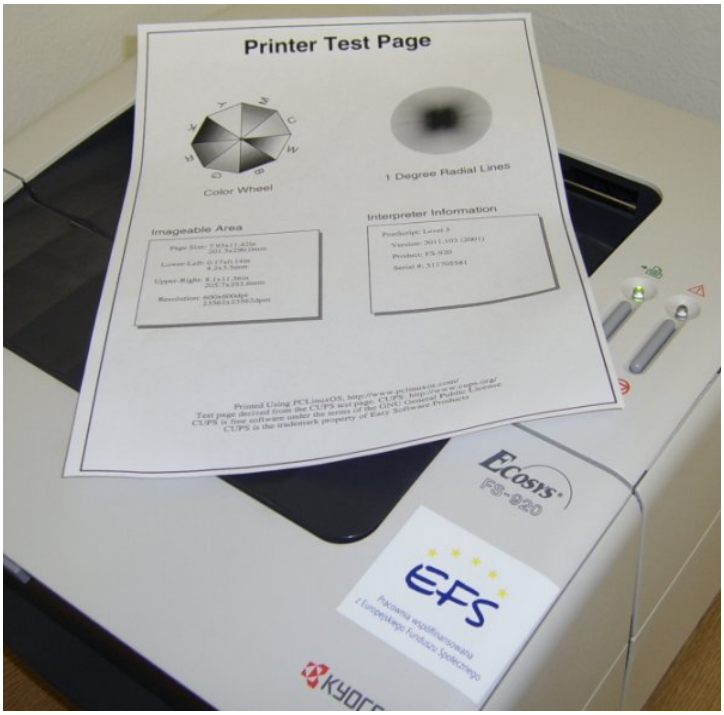


Rysunek 45: Krok drugi - wykrycie drukarki

Przeważnie kreator instalacji sam prawidłowo dobierze sterownik, jeśli nie wystarczy go wybrać z rozwijanej listy producentów i drukarek. Praktycznie na tym kończy się konfiguracja. Należy jeszcze tylko wydrukować stronę testową drukarki, żeby być pewnym, że wszystko działa prawidłowo. Łącznie cała procedura dodawania drukarki to trzy proste kroki (Rysunek 44: Krok pierwszy - dodaj nową drukarkę., *Rysunek 45: Krok drugi - wykrycie drukarki, Rysunek 46: Krok trzeci - zidentyfikowanie sterownika*)

Na komputerach z Linuksem dodajemy drukarkę w identyczny sposób. Komputery z Windows będą wymagały sterowników. Konfiguracja druku dla maszyn klienckich może być różna. Najprostsze będzie dodanie drukarki sieciowej bezpośrednio tak, jak na serwerze.



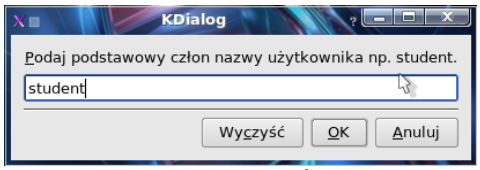


Rysunek 47: Tak wygląda strona testowa z drukarki FS-920 Kyocera.

Samba

EOS zawiera domyślnie skonfigurowaną Sambę z aktywną funkcją kontrolera domeny dla komputerów z *Windows*. Samba autoryzuje też hasła dla użytkowników stacji linuksowych. Aby przystąpić do pracy należy najpierw dodać użytkowników. Czynność tę przeprowadzamy za pomocą skryptów na serwerze. Administrator ma możliwość dodania pojedynczego użytkownika oraz zbiorowego według ustalonego wzorca. Dodając pojedynczego użytkownika – należy podać jego nazwę i hasło początkowe.

Zakładając grupę użytkowników zbiorowo (np. uczniów danej klasy), podać należy pierwszy, stały człon nazwy (*Rysunek 48: Skrypt dodawania użytkowników*). Skrypt zapyta następnie o ilość kont i do tej nazwy doda kolejno numery. Tak więc przy tworzeniu dziesięciu kont o podstawowej nazwie student, powstanie dziesięć loginów o nazwach od *student1* do *student10*. Trzeba będzie również podać hasło początkowe, które będzie dotyczyło całej tej grupy. Użytkownicy będą mogli zmienić to hasło, a zostało to opisane w części dotyczącej stacji roboczej.



Rysunek 48: Skrypt dodawania użytkowników

NIS i NFS

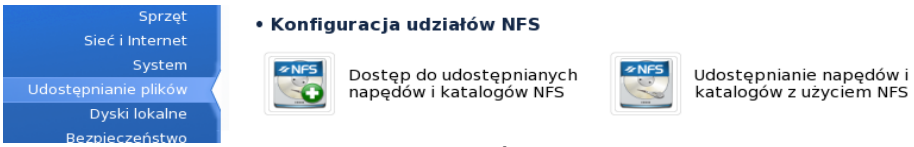
Stacje z systemem Linux wykorzystują NIS do logowania się na serwerze, a katalogi użytkowników montowane są przez usługę NFS. Dlatego przed rozpoczęciem pracy należy wykonać kilka czynności administracyjnych. Po założeniu kont użytkowników opisanym w poprzedniej części, należy uaktualnić bazę NIS. Wykonujemy to poleceniem make w katalogu */var/yp* (*Rysunek 49: Uaktualnienie bazy NIS*).

```
[guest@eos ~]$ su -
Password:
[root@eos ~]# cd /var/yp
[root@eos yp]# make
gmake[1]: Entering directory `/var/yp/school'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating shadow.byname...
Updating netid.byname...
# mail netgrp publickey networks ethers bootparams printcap \
        # amd.home auto.master auto.home auto.local passwd.adjunct \
        # timezone locale netmasks
gmake[1]: Leaving directory `/var/yp/school'
[root@eos yp]#
```

Rysunek 49: Uaktualnienie bazy NIS

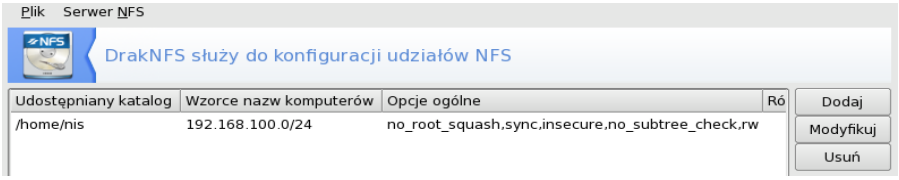
Tę czynność należy wykonać zawsze po dodaniu kolejnych użytkowników stacji klienckich. Należy tez sprawdzić, czy usługa dopuszczająca montowanie na stacjach katalogów serwera jest skonfigurowana i następnie skonfigurować ją na stacjach klienckich, co zostało opisane w rozdziale dotyczącym stacji z systemem Linux. Otwieramy w tym celu panel administracyjny (*Rysunek 50:*

Zakładka Udostępnianie plików) w zakładce *Udostępnianie plików* i wybieramy opcję *Udostępnianie napędów i katalogów...*



Rysunek 50: Zakładka Udostępnianie plików

Wpis, który zobaczymy powinien wyglądać tak, jak na rysunku (*Rysunek 51: Udostępnianie katalogu serwera*). Należy też pamiętać o sprawdzeniu, czy usługa NFS działa i wiedzieć, że jeśli zmieniliśmy zakres sieci LAN na inną klasę adresów, to w tym punkcie również trzeba dokonać modyfikacji.



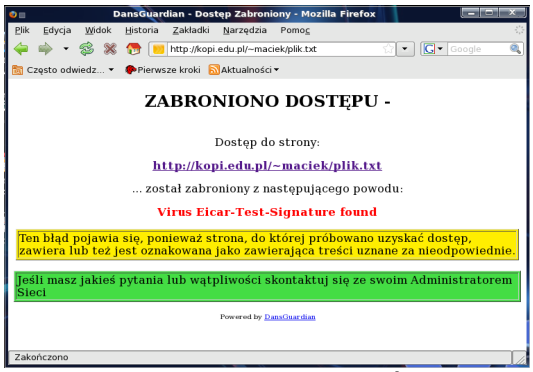
Rysunek 51: Udostępnianie katalogu serwera

Serwer FTP

Funkcję serwera FTP pełnie aplikacja ProFTPD. Serwer FTP nie wymaga konfiguracji. Jednak, aby mógł pracować należy dodać użytkowników wirtualnych (służy do tego ten sam panel, w którym dodaje się użytkowników wirtualnych poczty). Domyślnie nie ma na serwerze FTP dostępu anonimowego.

Ochrona antywirusowa

W systemie został zainstalowany program antywirusowy *Clamav*. Zapewnia on ochronę stacji roboczych z Windows dzięki współpracy z usługami *Dansguardian* (*Rysunek 52: Strona pojawiająca się podczas próby otwarcia zarażonego pliku*), *P3scan* i *Samba*. W ten sposób komputery są chronione przed wirusami, które mogą być w plikach ściąganych z internetu (www i poczta), a także w dużej mierze przed rozprzestrzenianiem się wirusów w obrębie sieci, dzięki skanowaniu folderów użytkownika „w locie”. Po otwarciu zarażonego pliku, użytkownik informowany jest o braku dostępu do pliku, a sam plik zostaje przeniesiony do folderu */tmp* na serwerze z przedrostkiem *vir-* w nazwie.



Rysunek 52: Strona pojawiająca się podczas próby otwarcia zarażonego pliku

Fail2ban

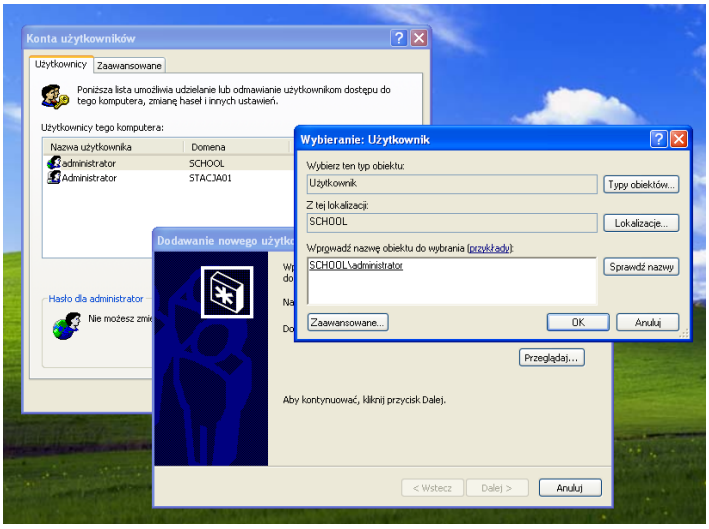
Jako zabezpieczenie przed sieciowymi atakami służy program Fail2ban. Domyślnie program jest uruchomiony i zabezpiecza usługę *ssh*, *httpd* i *ftp*. Działanie programu polega na wychwytywaniu z logów zdefiniowanych „złych” zachowań i blokowanie dostępu z takich numerów IP, z których te ataki następują. Szczególnie skutecznie zapobiega to skanowaniu serwera przez boty sieciowe, które używając losowych loginów, próbują znaleźć słabe punkty serwera. Ze względu na szybkość działania boty te mogą być dość uciążliwe, ponieważ zmuszają serwer do przetwarzania tych fałszywych loginów. Zwiększa to obciążenie systemu i znacznie lepszą alternatywą jest blokowanie takiego hosta.

Instalacja i konfiguracja stacji roboczej

Windows

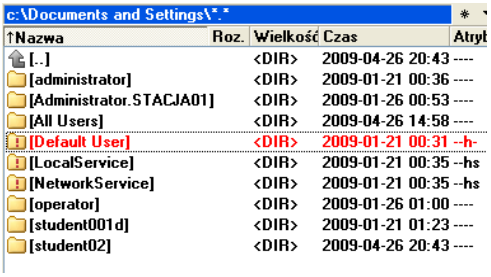
Instalacja systemu jest opisana w książeczkach dołączanych do systemu, więc w tym dokumencie zostanie jedynie przedstawiona konfiguracja w celu dołączenia do domeny i prawidłowej pracy.

Komputer z zainstalowanym systemem Windows najpierw należy uruchomić z uprawnieniami lokalnymi. W następnej kolejności dodajemy komputer do domeny, sprawdzamy prawidłowość dołączenia logując się na jedno z utworzonych na serwerze kont. Konfigurujemy to konto, możemy np. ustawić tapetę, jaka użytkownicy powinni widzieć na pulpicie oraz inne elementy systemu. Należy też pamiętać o zainstalowaniu wszystkich potrzebnych do pracy programów. Jest to szczególnie istotne, jeśli zamierzamy wykonać potem obraz systemu i przenieść go na inne komputery. Następnie ponownie logujemy się lokalnie z uprawnieniami administratora. Teraz dodajemy administratora sieciowego, jako administratora tego komputera (*Rysunek 53: Administrator domeny na lokalnym komputerze*).



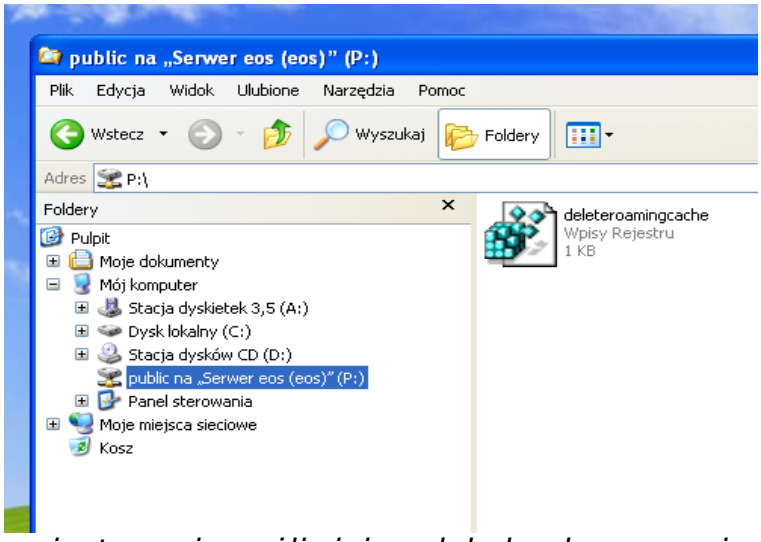
Rysunek 53: Administrator domeny na lokalnym komputerze

W kolejnym kroku należy się zalogować jako administrator domeny. Warto mieć zainstalowany menedżer plików, który pokazuje katalogi i pliki ukryte (*Rysunek 54: Ukryty katalog Default User*). Aby każdy następny użytkownik miał ustawienia identyczne, jak ten przez nas skonfigurowany, trzeba kilka plików skopiować na serwer.Jest to przede wszystkim katalog *Default User* w całości oraz plik *NTUSER.DAT* z katalogu skonfigurowanego przez nas użytkownika. Katalog umieszczamy na serwerze w */home/samba/netlogon*, a w nim plik *NTUSER.DAT*.

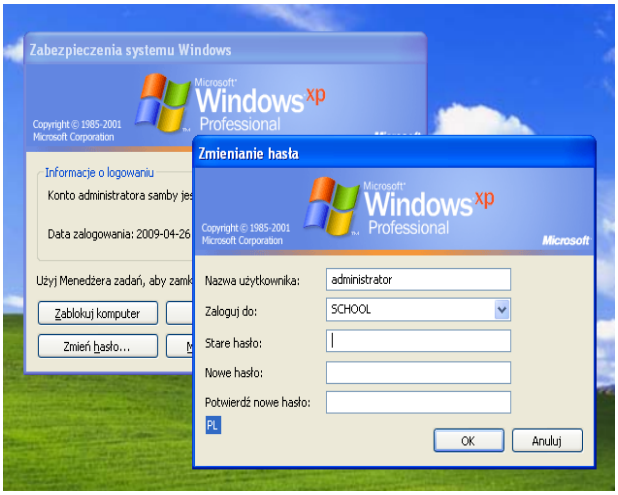


Rysunek 54: Ukryty katalog Default User

Można dodać z katalogu *public* na serwerze wpis rejestru (*Rysunek 55: Plik rejestru uniemożliwiający lokalne keszowanie profili*), który zapobiegnie tworzeniu się lokalnych kopii profilu sieciowego. w tym celu trzeba być zalogowanym jako administrator. Ponieważ hasła użytkowników na serwerze są identyczne dla wszystkich, a i administrator domeny ma hasło standardowe, należy pamiętać, aby po pierwszym zalogowaniu każdy użytkownik zmienił hasło. W tym celu trzeba wcisnąć klawisze *ctrl+alt+del* i wybrać opcję *Zmień hasło...*(*Rysunek 56: Zmiana hasła uzytkownika*)



Rysunek 55: Plik rejestru uniemożliwiający lokalne keszowanie profili



Rysunek 56: Zmiana hasła uzytkownika

Linux

Informacje na temat stacji linuksowej podzielone są na dwie zasadnicze części. W pierwszej zostanie opisana instalacja systemu z płyty DVD, w drugiej zaś konfiguracja systemu oraz czynności konfiguracyjne związane z dodaniem komputera do domeny.

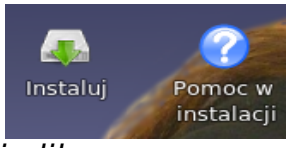
Uruchomienie z płyty DVD

Uruchamiamy komputer z płyty DVD, jeśli na komputerze nie ma zainstalowanego systemu stanie się to automatycznie, w przeciwnym wypadku może być konieczne ustawienie w BIOSie maszyny, aby start odbywał się najpierw z nośnika optycznego. Podczas uruchamiania systemu należy potwierdzić układ klawiatury *polski (programisty)* (*Rysunek 57: Zmień układ klawiatury na polski*).

Rysunek 57: Zmień układ klawiatury na polski

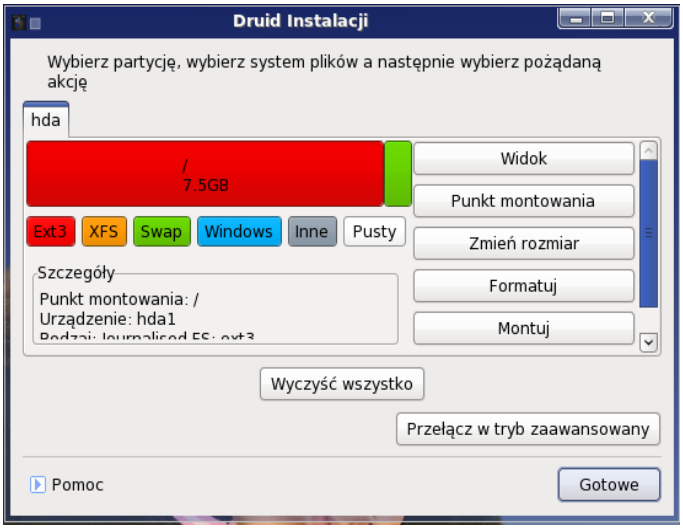
Instalacja na dysku

Po uruchomieniu systemu należy przeczytać informację umieszczoną na pulpicie i przystąpić do instalacji. Na pulpicie znajdują się dwie ikony – skrót do pliku z pomocą i skrót do programu instalacyjnego (*Rysunek 58: Ikony - instalator i plik pomocy*).



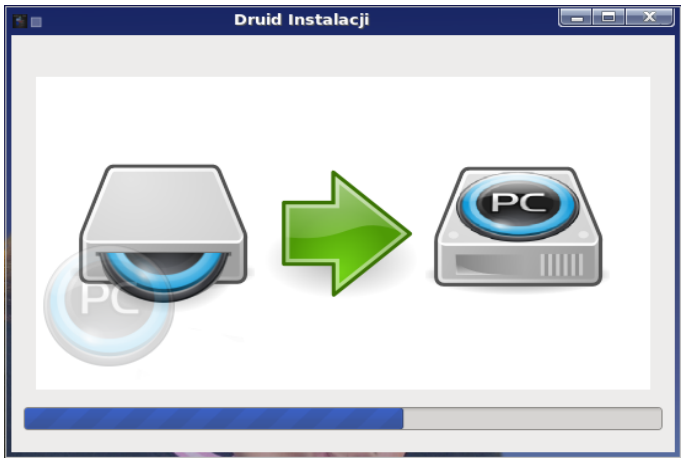
Rysunek 58: Ikony - instalator i plik pomocy

Należy kliknąć ikonę pomocy i przeczytać dokładnie informacje tam zawarte. Okno pomocy można zostawić otwarte podczas instalowania systemu i sprawdzać kolejno wykonywane czynności (*Rysunek 59: Okno ręcznego podziału dysku na partycje, Rysunek 60: Okno z paskiem postępu instlacji, Rysunek 61: Okno instalacji bootloadera - GRUB*).



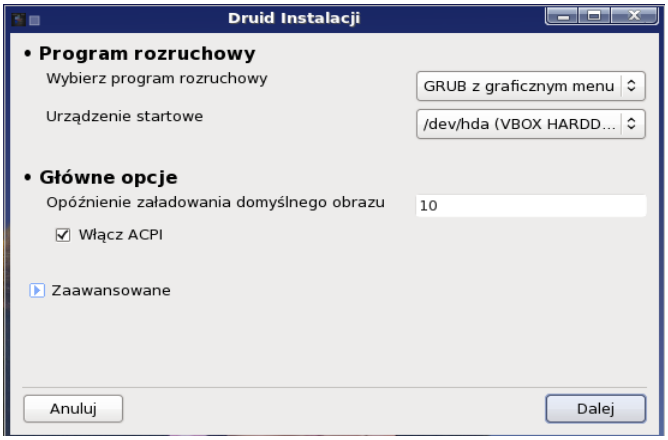
Rysunek 59: Okno ręcznego podziału dysku na partycje

Spośród opcji przygotowania dysku najlepiej wybrać „*Samodzielne partycjonowanie dysku*”, ponieważ wówczas dokładnie można zaplanować rozmiar poszczególnych partycji, a dysk jest czytelnie zobrazowany w formie blokowego wykresu.
Po założeniu partycji i kliknięciu przycisku „Gotowe”, pojawi się okno postępu instalacji.



Rysunek 60: Okno z paskiem postępu instlacji

Na koniec zostanie zainstalowany program rozruchowy, czyli bootloader. Podczas instalacji lub później można zmienić tzw. etykietę, zostało to opisane w końcowej części dokumentu.



Rysunek 61: Okno instalacji bootloadera - GRUB

Jeśli chcemy mieć komputer dwusystemowy i zachować Windows, lepiej wcześniej użyć preferowanego przez siebie programu do zmniejszenia partycji FAT lub NTFS.

Można zastosować uruchomienie komputera z PXE i wykorzystać system ładowany z serwera – *Pmagic*, a w nim program *Gparted* (*patrz: uruchamianie z pxe*). Na nowym komputerze najpierw należy zainstalować *Windows*, a potem *Linuksa*. W przypadku, gdy *Linux* będzie jedynym systemem, można wykorzystać cały dysk. Najlepiej wybrać opcję *Custom partitioning* (Własne partycjonowanie), ponieważ widać wtedy cały dysk w formie wykresu. Partycję swap należy założyć, jeśli komputer ma 512 MB RAM, przy 1 GB lub więcej nie jest to potrzebne. Jeśli chcemy przeznaczyć na dane osobną partycję, trzeba pamiętać, ze na system potrzebujemy około 10 GB. Ponieważ uczniowie będą się logować do serwera i korzystać z jego zasobów, nie jest to niezbędne. Należy rozważyć, czy będziemy chcieli robić własny obraz systemu np. po dodaniu nowych programów. Jeśli tak, to partycja systemowa powinna mieć około 20 GB, żebyśmy byli pewni, ze własny obraz nam się na niej zmieści bez problemów. Obecnie dyski są bardzo duże w stosunku do potrzeb szkolnych, więc możemy przeznaczyć odpowiednio więcej miejsca na *Linuksa* (jeśli partycja będzie odpowiednio duża, możemy w przyszłości na niej zrobić kopię

zapasową *Windows* i przywracać ją w razie zawirusowania). W takim przypadku przynajmniej jedna z linuksowych partycji powinna być większa niż powierzchnia zajmowana przez *Windows*.

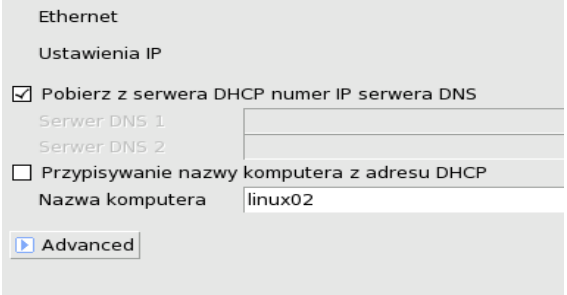
Ważne! Aby zarządzanie stacjami było bezproblemowe, spisujemy *MAC* karty sieciowej i dodajemy komputer w konfiguracji *DHCP* na serwerze, tak aby zawsze dostawał ten sam IP z określoną nazwą np. stacja01. Po tej czynności restartujemy usługę *DHCP*, sprawdzamy, czy odbyło się to poprawnie i dopiero wtedy zamykamy system na stacji roboczej, klikając „*Uruchom komputer ponownie*".

Pierwsze uruchomienie

Po ponownym uruchomieniu komputera należy wykonać kilka czynności wstępnych. Najpierw ustalamy hasło roota (*Rysunek 62: Ustawienie hasła roota i dodanie użytkownika stacji roboczej*). Dla ułatwienia takie same hasło możemy mieć na wszystkich stacjach roboczych. Jednak lepiej, aby nie było to takie samo hasło, jak do serwera. Będzie ono potrzebne tylko do zadań administracyjnych, takich, jak instalacja nowego oprogramowania i ewentualnie usuwania błędów, jakie mogą się pojawić na stacji lokalnej.

Rysunek 62: Ustawienie hasła roota i dodanie użytkownika stacji roboczej

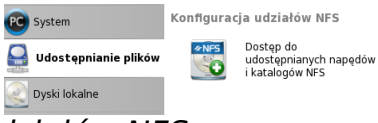
Hasło roota nie powinno być hasłem łatwym – słownikowym. Choć system będzie korzystać z kont na serwerze, musimy też założyć konto użytkownika, w przeciwnym razie nie będzie możliwe dokończenie konfiguracji. Pierwszy raz logujemy się jako root z ustawionym przed chwilą hasłem. Pomimo pojawienia się ostrzeżenia „*Access Denied*" logowanie przebiegnie poprawnie. Nie należy potem juz nigdy logować się na konto roota. Teraz wykonujemy kilka czynności konfiguracyjnych w celu aktywowania logowania zdalnego. Należy komputerowi przypisać niepowtarzalną nazwę. W konfiguracji komputera przeprowadzamy konfigurację nowego łącza. Wybieramy kartę sieciową,



Rysunek 63: Konfiguracja sieci na stacji roboczej

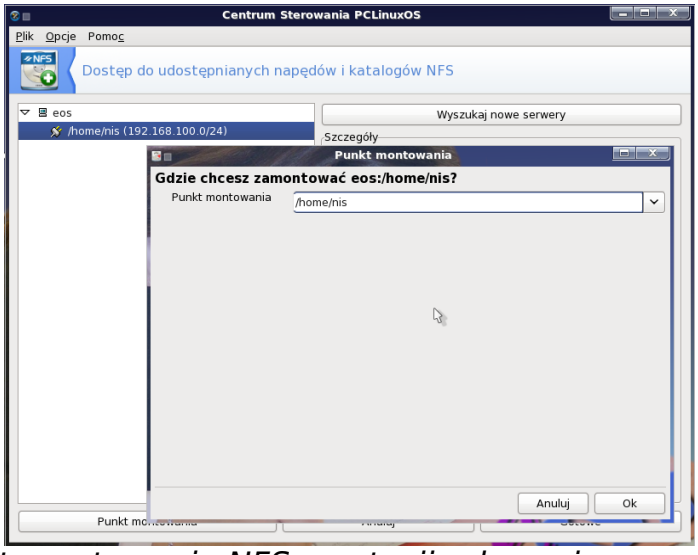
każemy systemowi korzystać z klienta *DHCP* i wpisujemy nazwę (*Rysunek 63: Konfiguracja sieci na stacji roboczej*). Jeśli tego nie zrobimy, komputer będzie

identyfikowany jako localhost i powstanie problem z dołączeniem do domeny, jeśli w kolejnej stacji też pominiemy tę czynność. Ponieważ klient linuksowy korzysta z Samby tylko jako serwera haseł, będzie można się zalogować, gdyż serwerem samej autoryzacji jest NIS. Jednak nie będzie autoryzacji maszyny i w ten sposób odcięte zostaną zasoby Samby na serwerze i np. otoczenie sieciowe komputerów z Windows. Będzie się też pojawiało okno z błędem podczas logowania.



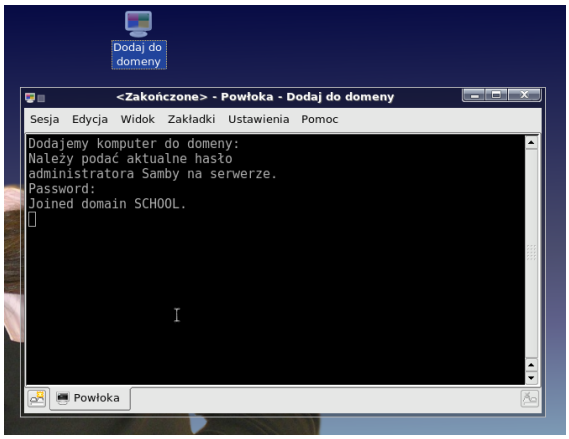
Rysunek 64: Konfiguracja udziałów NFS

Uruchamiamy panel *Konfiguracja komputera* i w zakładce *Udostępnianie plików* wybieramy *Dostęp do udostępnianych napędów i katalogów NFS*. Należy kliknąć *Szukaj serwerów* i poczekać, aż serwer zostanie odnaleziony, kolejno rozwinąć opcje klikając



Rysunek 65: Punkt montowania NFS na stacji roboczej

nazwę serwera, a potem kliknąć *Punkt montowania*. Jako miejsce montowania wybieramy */home/nis* i potwierdzamy decyzję o zapisaniu konfiguracji w pliku *fstab* (*Rysunek 64: Konfiguracja udziałów NFS, Rysunek 65: Punkt montowania NFS na stacji roboczej*). Kolejna czynność to dodanie komputera do domeny. Ikona skryptu znajduje się na pulpicie roota. Klikamy ją i w okienku terminala podajemy hasło administratora domeny oraz potwierdzamy je enterem. Należy być pewnym, że nazwa komputera została ustawiona.



Rysunek 66: Konsolowy, ale prosty skrypt dodawania do domeny

Po zobaczeniu napisu *Joined domain SCHOOL*, okno można zamknąć (*Rysunek 66: Konsolowy, ale prosty skrypt dodawania do domeny*). Teraz jeszcze należy usunąć użytkownika, którego tymczasowo trzeba było założyć podczas instalacji i zrebootować system. Konto usuwamy, wybierając z menu: *System – Konfiguracja – Konfiguracja komputera*. W oknie, które się pojawi, klikamy zakładkę *System* i dalej *Zarządzanie użytkownikami*. Od tego momentu można się już logować do domeny.

Jeśli komputer został już skonfigurowany i sprawdziliśmy prawidłowe logowanie do domeny, można lepiej dostroić system. Warto przejrzeć repozytorium pakietów i zainstalować te, które naszym zdaniem w codziennej pracy szkolnej mogą się przydać. W usługach można wyłączyć te, które są niepotrzebne, a przede wszystkim usługę *dkms*, która ma za zadanie budowanie sterowników w przypadku dołączenia nowego sprzętu.

Część konfiguracji można przeprowadzić z uczniami podczas ich pierwszego logowania, może to być np. zrobienie użytecznych skrótów do często wykorzystywanych aplikacji na pulpicie. Może to być zainstalowanie dodatków do przeglądarki Firefox. Ważne jest też, aby użytkownicy zmienili swoje hasła ze standardowych, które powstały na etapie zakładania kont. Skrót do zmiany hasła przez użytkowników linuksowych jest umieszczony w menu *System*.

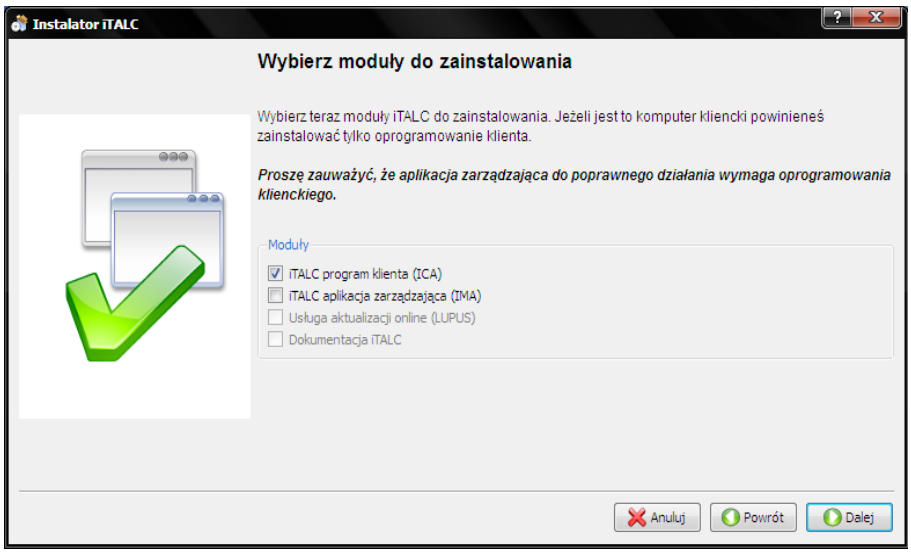
Katalogi domowe użytkowników stacji Windows znajdują się w */home/samba/profiles* – na serwerze. Katalogi uczniów pracujących na Linuksie są w */home/nis* również na serwerze.

Interesujące dodatki

Kontrola stacji programem iTALC

Instalacja i konfiguracja

Użytkownicy systemu **EOS** otrzymują program iTalc wraz systemem. Jedynie ci, którzy będą używać stacji roboczych z Windows (lub z innymi dystrybucjami Linuksa), muszą zainstalować go sami. Większość dystrybucji Linuksa zawiera w repozytoriach

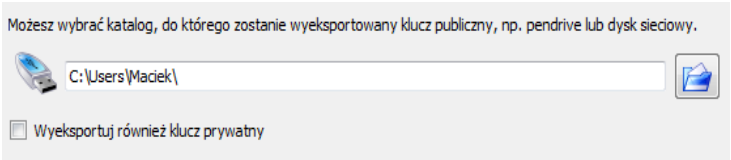


Rysunek 67: Instalator programu iTALC

pakiet *iTalc*, zatem można go łatwo zainstalować za pomocą menedżera pakietów. W systemie Windows jest również łatwy w użyciu instalator (*Rysunek 67: Instalator programu iTALC*). Trzeba pamiętać, że program instaluje się na wszystkich komputerach. Na

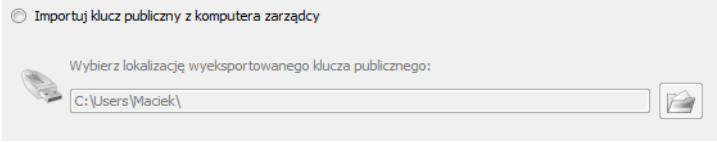
stacjach klienckich oprogramowanie klienta, a na serwerze kontrolującym (może być to serwer w pracowni lub komputer nauczyciela) także aplikację zarządzającą. Od serwera trzeba zacząć. Program jest rozprowadzany na licencji GPL i przed instalacją trzeba potwierdzić swoją zgodę na warunki licencji. Potem wybrać katalog instalacyjny, warto pozostawić ten zaproponowany domyślnie. W przypadku komputera zarządzającego zaznaczamy „*iTALC program klienta (ICA)*” oraz „*iTALC aplikacja zarządzająca (IMA)*”. Na stacjach roboczych należy wybrać tylko pierwszą z opcji.

Podczas instalacji modułu zarządzania należy wybrać opcję wygenerowania nowej pary kluczy – publicznego i prywatnego. W Ubuntu zostanie to zrobione automatycznie, zaś w innych Linuksach trzeba w konsoli (jako root) wpisać polecenie *ica -role teacher -createkeyipair*. W Windows pojawi się to jako jedna z opcji instalacji.Pod koniec należy wybrać odpowiedni katalog, w którym zostanie zapisany wyeksportowany klucz publiczny(*Rysunek 68: Eksport klucza publicznego*). Jest to plik *italc_dsa_key.pub* i musi być dostępny na komputerach z aplikacją klienta. W **EOS** znajdziemy ten klucz na pulpicie w katalogu *Dokumentacja*.



Rysunek 68: Eksport klucza publicznego

Na stacjach roboczych instalujemy tylko program klienta. Wcześniej wygenerowane klucze musimy umieścić w lokalizacji sieciowej dostępnej dla maszyn w sieci lub skopiować na dysk przenośny. Podczas instalacji nie generujemy nowych kluczy tak jak na komputerze zarządzającym, ale wybieramy opcje importu, jak na rysunku poniżej (*Rysunek 69: Skąd skopiować klucz publiczny?*).



Rysunek 69: Skąd skopiować klucz publiczny?

Konfiguracja polega głównie na dodaniu pracowni (może być ich kilka), a następnie pojedynczych komputerów. Będziemy potrzebować adresy MAC wszystkich komputerów. W sieci linuksowej dzięki odpowiedniej konfiguracji statycznych IP w *DHCP* oraz pliku */etc/hosts*, można użyć numerów IP lub nazw, jakie zostały nadane maszynom. W sieci z serwerem *SBS* należy użyć raczej nazw typu *STACJA01*, niż IP, ponieważ te ostatnie mogą się zmieniać. Oczywiście możemy też nadać stałe IP komputerom, co jest jednak trudniejsze.

Każdy komputer może mieć jeszcze inną nazwę widoczną tylko w programie iTalc, musimy znać jego *MAC* i określić jego przynależność do grupy stacji uczniowskich lub komputerów personelu. Wszystkie dodane komputery będą nam się pojawiać w oknie programu zarządzającego. W zasadzie najlepszą i najłatwiejszą opcją jest instalacja programu zarządzającego w każdej pracowni. Można jednak pokusić się o centralną taka aplikację w szkole. Wymagać to jednak będzie odpowiedniego przekazywania portów 5800 i 5900, co na serwerze *SBS* nie jest sprawą trywialną.

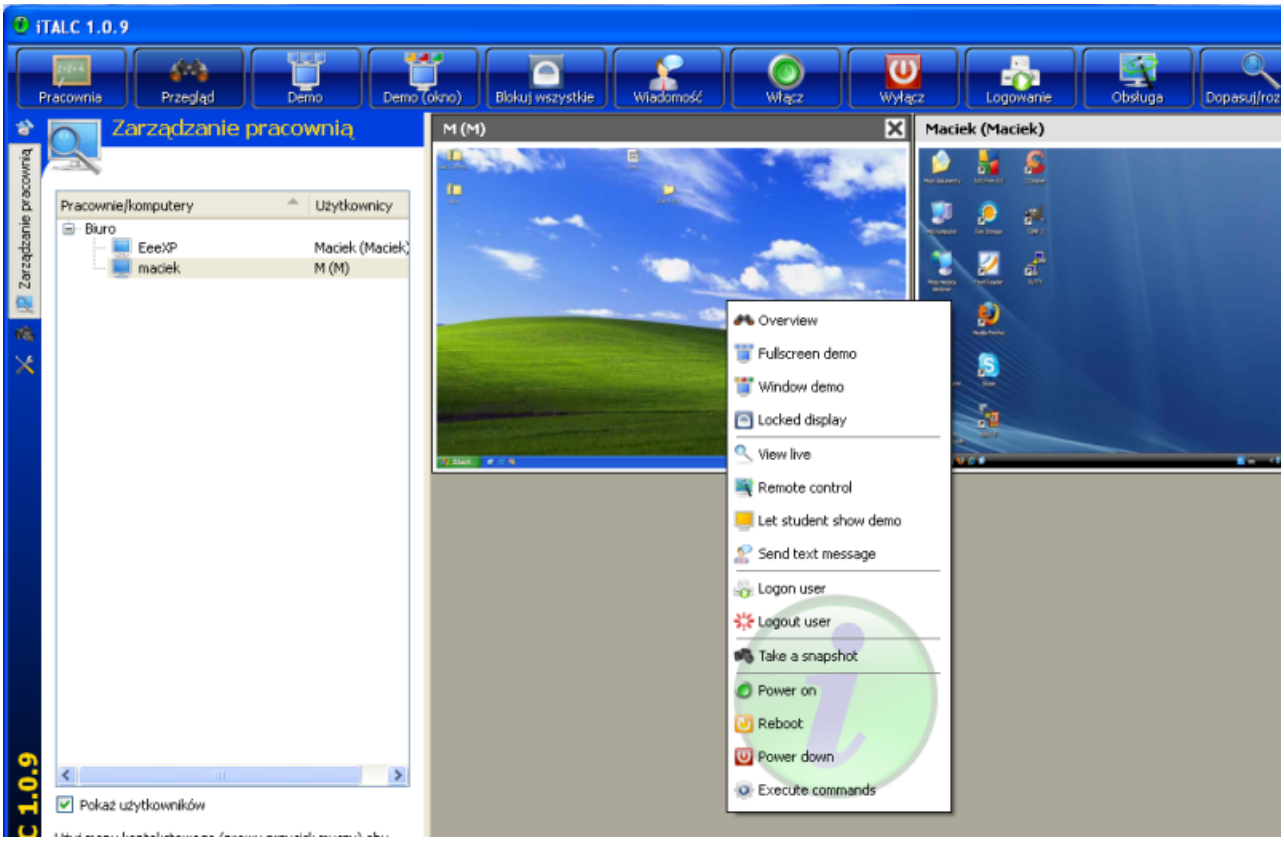
Program bez problemu działa na systemach linuksowych oraz na *Windows 2000*, a także *XP*. Jednak w przypadku zastosowania zapory może być konieczne dodanie programu do wyjątków, szczególnie wtedy gdy zapora wcześniej była konfigurowana

niestandardowo. System *Windows Vista* nie jest przystosowany do działania programu. Problemem jest tzw. *UAC*, czyli mechanizm zabezpieczeń wymagający potwierdzania chęci uruchomienia programów nieuznawanych przez system jako wiarygodne.

Pomimo dodania *iTalc* do usług, program nie działa prawidłowo, jednak można to obejść kosztem kilku funkcji programu. Po pierwsze należy *iTalc* dodać do wyjątków w zaporze *Windows*. Następnie w *Eksploratorze Windows* przechodzimy do katalogu programu w *Program files*. Klikamy prawym klawiszem na ikonie programu, wybieramy *Właściwości* i zakładkę *Zgodność*, a tam zaznaczamy opcję „*Uruchom ten program w trybie zgodności z: Windows XP...*" Kolejny krok to dodanie programu do *Autostartu*. Klikając prawym klawiszem na *Autostart* w *Menu*, wybieramy opcję „*Eksploruj wszystkich użytkowników*" i tam przenosimy wcześniej utworzony skrót do programu. Należy to wykonać z poziomu administratora komputera. Po ponownym zalogowaniu zapewne pojawi się okno z pytaniem, czy uruchomić program, należy wówczas odznaczyć opcję pytania za każdym razem i zatwierdzić. Dopiero w kolejnych logowaniach program będzie się uruchamiał całkowicie automatycznie. W systemie Windows Vista nie będzie możliwe zdalne zalogowanie przez konsolę iTalc, pozostałe funkcje działają raczej prawidłowo.
Również Linux wymaga, aby aplikacja klienta uruchamiana była automatycznie. Można to uzyskać dwoma sposobami – podobnie jak w Windows skorzystać z automatycznego startu po logowaniu lub uruchomić program jako usługę systemową.

Zarządzanie

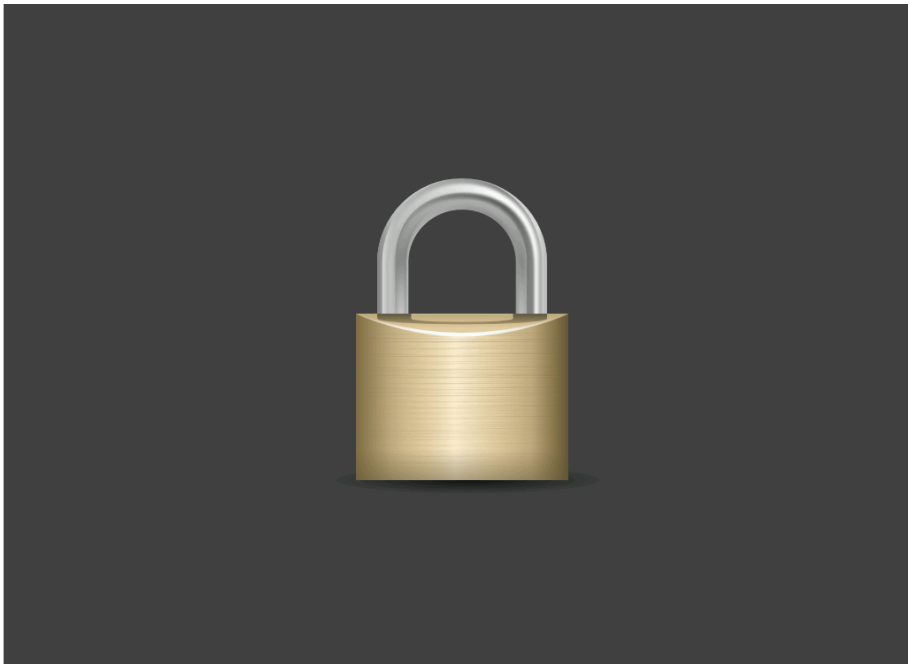
Konsola zarządzania jest prosta (*Rysunek 70: Konsola zarządzania programu iTALC*), pomimo tego, że nie wszystkie elementy zostały przetłumaczone na język polski (dotyczy to systemu Windows).



Rysunek 70: Konsola zarządzania programu iTALC

Możliwości programu i jego prostota pozwalają na zarządzanie nawet przeciętnemu użytkownikowi. Zatem można to narzędzie udostępnić nauczycielom innych przedmiotów i lepiej by było zainstalowane tak, aby ci nauczyciele mogli z niego korzystać. Z tego względu raczej nie należy go instalować na serwerze SBS. Za to bez obaw można założyć konta użytkowników na serwerze linuksowym. Dobrze byłoby oczywiście przeprowadzić krótkie szkolenie dla nauczycieli, aby mogli z tego narzędzia korzystać podczas lekcji.
iTalc jest odpowiedzią na jeden podstawowy problem związany z prowadzeniem innych niż informatyka lekcji. Nauczyciele zwykle obawiają się, że nie będą panować nad tym, co robią uczniowie, że zamiast np. zrobić notatkę będą w tym czasie korzystać z komputera w sposób niezwiązany z lekcją. Możliwość blokowania stacji zapobiega takiej ewentualności. Dodatkową zaletą jest to, że nauczyciel obserwuje prace stacji na miniaturkach i w każdej chwili może powiększyć podgląd dowolnej z nich, działania nauczyciela nie są w żaden sposób komunikowane komputerom klienckim i uczeń nie wie o tym, że jest obserwowany. Program umożliwia włączanie (o ile sprzęt posiada funkcję WOL) i wyłączanie komputerów. Można jednym kliknięciem włączyć lub wyłączyć całą pracownię lub pojedynczą stację. Można się też zdalnie zalogować lub wylogować użytkownika.

Wszystkim lub pojedynczym użytkownikom można wysłać wiadomość, która w osobnym okienku pojawi się na ekranie. Można też wszystkim lub pojedynczemu użytkownikowi zablokować dostęp do funkcji systemu (*Rysunek 71: Zablokowany ekran stacji roboczej*). Zobaczy on wówczas rysunek kłódki na ekranie i nie będzie mógł odblokować działania pulpitu, jest to przydatne wówczas, gdy nauczyciel chce objaśnić zagadnienia wymagające uwagi uczniów.



Rysunek 71: Zablokowany ekran stacji roboczej

Ponadto ciekawą opcją jest tryb demo. Podczas pełnoekranowego trybu demo uczeń nie ma możliwości wykonywania innych czynności. Nauczyciel może pokazać np. funkcje jakiegoś programu wszystkim uczniom, taką samą funkcję może udostępnić wybranemu uczniowi. Z poziomu aplikacji można też przejąć kontrolę nad dowolnym komputerem, użytkownik staje się wówczas tylko obserwatorem własnego pulpitu. Istnieje też opcja pomocy zdalnej, nie odbiera się użytkownikowi panowania nad myszką i klawiaturą, ale można mu pomóc w wykonaniu trudniejszych czynności.

Program jest łatwy w instalacji i konfiguracji oraz prosty w użytkowaniu. Warto dać takie narzędzie wszystkim pracującym z młodzieżą. Działanie w sieci LAN nie powoduje jej nadmiernego obciążenia. Dodatkową zaletą jest możliwość używania programu zarówno na komputerach z Windows, jak i z Linuksem. Niewątpliwą zaletą jest licencja GPL i możliwość bezpłatnego używania programu.

Bibliografia:

1. *Linux Magazine, nr 59, styczeń 2009*
2. *http://italc.sourceforge.net*

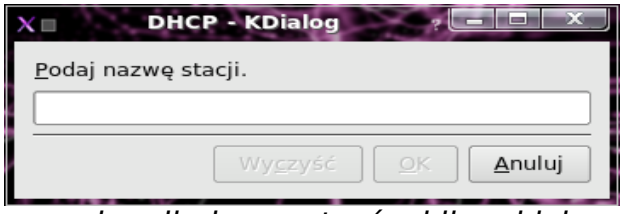
Statyczne wpisy DHCP

Serwer *DHCP* przydziela stacjom roboczym numery IP oraz wskazuje, jakie są dodatkowe parametry połączenia: brama, maska, serwery nazw i kilka innych jeszcze danych. Aby administrator miał łatwiejszą pracę, warto podczas konfiguracji sieci zająć się sporządzeniem statycznych wpisów *DHCP*. Minimalny wpis dla pojedynczego hosta, przy założeniu, że wszystkie potrzebne parametry zostały zdefiniowane w sekcji ogólnej pliku *dhcpd.conf*, wyglądać może następująco.

stacja01 {
hardware ethernet 00:E0:4C:89:3B:41;
fixed-address 192.168.100.4;
}

Oznacza on, że komputerowi o konkretnym adresie fizycznym karty (*MAC*) zostanie przypisany zawsze ten sam numer IP. Jest to ważne np. dla sprawnej pracy programu *iTALC*, w przypadku wyjątków w regułach *Dansguardiana*, ale też dla diagnozowania ewentualnych problemów w sieci i utrzymania porządku.

Dodawanie wpisów dla poszczególnych maszyn odbywa się przez prosty okienkowy skrypt, w którym podajemy trzy zmienne: nazwę maszyny, adres MAC oraz numer IP*(Rysunek 72: Statyczne wpisy dla komputerów klienckich.).*



Rysunek 72: Statyczne wpisy dla komputerów klienckich.

Zdalny dostęp do serwera

Najprostszym sposobem skorzystania ze zdalnej pracy jest protokół *SSH*. W *Linuksie* otwieramy konsolę i wpisujemy:

```
[user@localhost~] ssh nazwa@moj.eos.serwer.pl
```

Pojawi się pytanie o hasło:

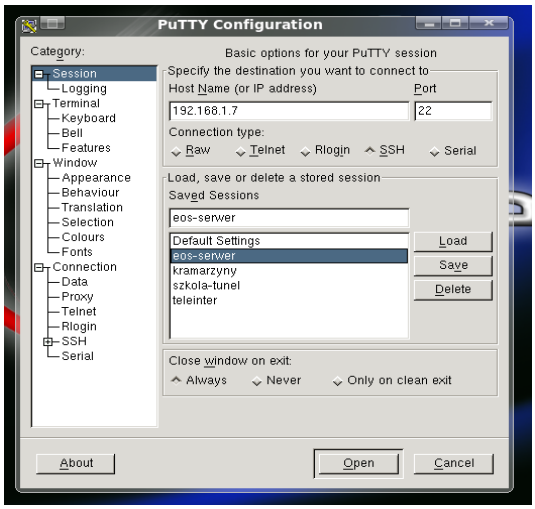
```
Password:
```

Po wpisaniu zobaczymy:

```
========================
     serwer eos
========================
[nazwa@serwer~]
```

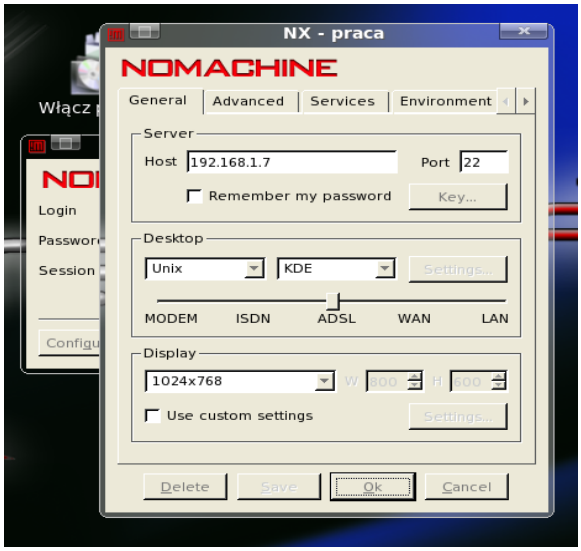
W Windows musimy użyć programu *PuTTy*, który jest dość prosty w konfiguracji.W pole *Host Name* wpisujemy adres serwera lub IP w polu *Saved Sessions* własną nazwę sesji, klikamy *Save*, aby na przyszłość nie wpisywać tego ręcznie (*Rysunek 73: Okno konfiguracji programu PuTTy*).

Aby rozpocząć połączenie należy kliknąć *Open*. Przez *SSH* możemy korzystać z programów należących do grupy *CLI* (*Command Line Interface*). Zaletą pracy zdalnej przez *SSH* jest mała ilość przesyłanych danych, a więc nawet na kiepskich łączach (np. *GPRS*) możemy się połączyć z serwerem i skontrolować najważniejsze jego parametry.



Rysunek 73: Okno konfiguracji programu PuTTy

Znacznie większy komfort pracy zapewnia połączenie przy pomocy programu *NX*. Aby z niego skorzystać, należy pobrać pakiet (lub plik instalacyjny) klienta ze strony *http://nomachine.com*. *NX* zapewni nam połączenie podobne jak tzw. pulpit zdalny w *Windows*. Niezależnie czy korzystamy z *Linuksa* czy z *Windows*, możemy skorzystać z tego programu. Jego zaletą jest dobra kompresja danych, więc można pracować nawet dysponując łączem o przepustowości 128 kilobitów.

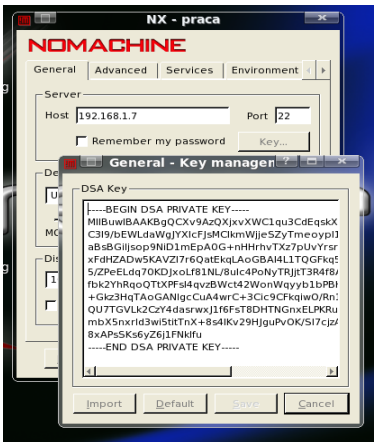


Rysunek 74: Okno konfiguracji klienta NX

Po uruchomieniu programu pierwszy raz należy go skonfigurować (*Rysunek 74: Okno konfiguracji klienta NX*). W pole *Host* wpisujemy adres lub IP (port podobnie jak w SSH to 22), jako *Desktop* wybieramy Unix i KDE, a rozdzielczość ekranu 1024x768 (im większa rozdzielczość, tym więcej danych).
Następnie klikamy przycisk *Key* i podajemy ścieżkę do pliku *server.id_dsa.key*, który wcześniej zapisaliśmy z serwera np. na pendrive (*Rysunek 75: Import klucza publicznego*).

Po kliknięciu przycisku *Import*, podaniu odpowiedniej ścieżki do klucza i

zatwierdzeniu przez naciśnięcie przycisku *Save* w okienku *Key management* zobaczymy zapis tego klucza. Teraz już po nadaniu jakiejś przyjaznej nazwy połączeniu, np. praca, możemy rozpocząć połączenie z serwerem (*Rysunek 76: Inicjowanie połączenia NX*).

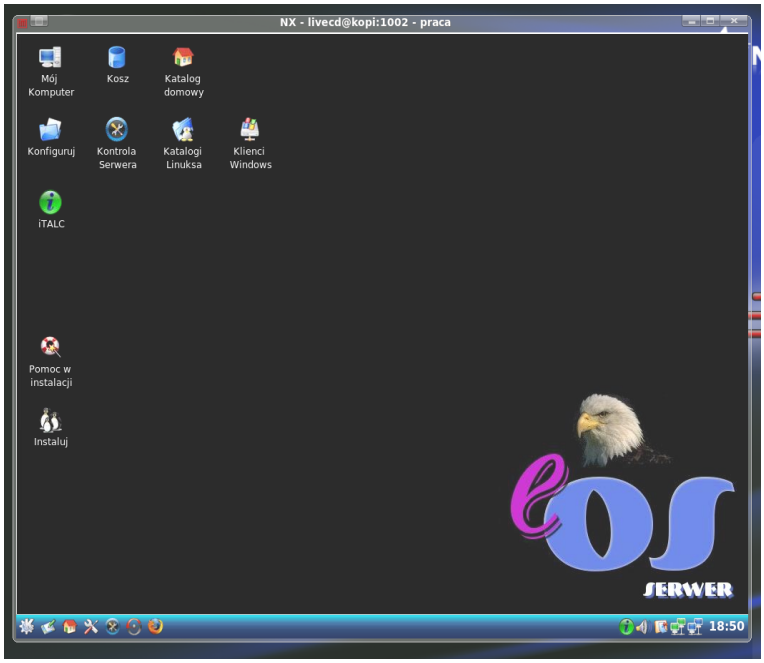


Rysunek 75: Import klucza publicznego

Po wpisaniu nazwy i hasła i kliknięciu *Login* zobaczymy po chwili pulpit zdalnego serwera.

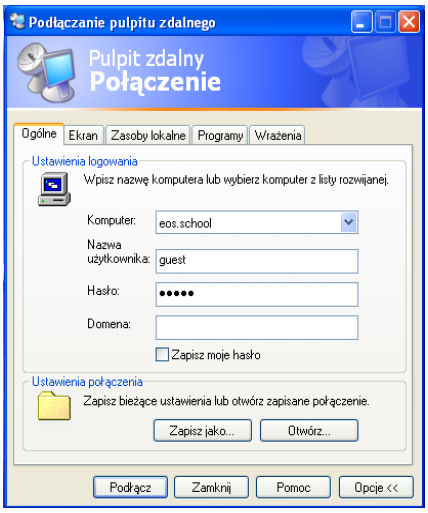
Rysunek 76: Inicjowanie połączenia NX

Jeśli użytkownik nie wylogował się wcześniej w lokalnie, to może zobaczyć podczas zdalnego połączenia błąd programu *ica* (klient *iTalc*), ponieważ zdalna sesja próbuje uruchomić program drugi raz. Mogą się tez pojawić błędy uruchomienia podsystemu dźwięku, ale nie ma to wpływu na zdalną pracę.



Rysunek 77: Zdalny pulpit NX

Inny sposób zdalnego połączenia z serwerem to wykorzystanie programu *XRDP*. Nie jest to opcja szczególnie polecana, bowiem wymaga otwarcia portu dla usługi (3389) i wymaga lepszego połączenia z powodu większej ilości przesyłanych danych. Bardziej nadaje się do wykorzystania w sieci lokalnej niż przez internet. Zaletą tego sposobu połączenia jest brak konieczności instalowania czegokolwiek po stronie klienta z *Windows* (co najmniej *XP*). Jeśli będziemy chcieli korzystać z tego programu, należy usługę włączyć w panelu administracyjnym (domyślnie jest wyłączona). Na komputerze klienckim wybrać należy z menu *Podłączenie pulpitu zdalnego*. Należy wpisać adres serwera, login użytkownika na serwerze i jego hasło (*Rysunek 78: Połączenie RDP z serwerem*).



Rysunek 78: Połączenie RDP z serwerem

Po kliknięciu przycisku Podłącz rozpocznie się połączenie i po chwili na ekranie Windows pojawi się pulpit serwera (*Rysunek 79: Zdalny pulpit serwera na pulpicie Windows*). Dobrze jest również w zakładce Ekran wybrać odpowiednią rozdzielczość i głębię kolorów. Przy maksymalnych ustawieniach ilość danych w sieci będzie dość duża, przy szybkości połączenia poniżej 256kbps spowoduje to „czkawkę” w przesyłaniu danych.

Rysunek 79: Zdalny pulpit serwera na pulpicie Windows

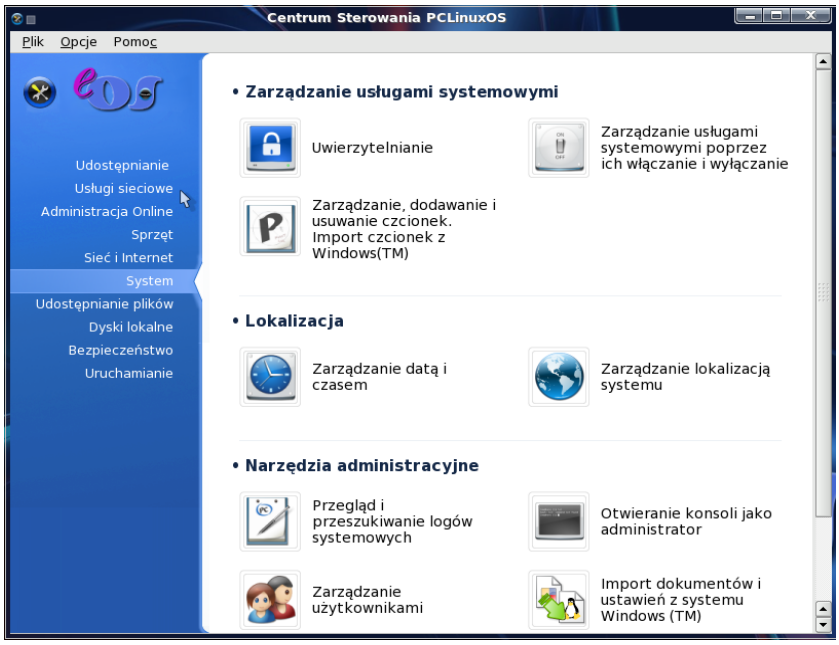
Jak już wcześniej wspomniano, użytkownik, który ma mieć dostęp przez *ssh* lub *nx*, musi zostać dopisany do dyrektywy *AllowUsers* w pliku */etc/ssh/sshd_config*. Autorzy

systemu założyli, że powinien to być jeden użytkownik. Na pulpicie znajduje się ikona uruchamiająca skrypt, który dodaje odpowiedni wpis. Skrypt ten będzie skuteczny tylko jeden raz, później ikonę z pulpitu należy usunąć. jeśli dostęp do systemu ma mieć większa liczba użytkowników, należy plik konfiguracyjny *ssh* edytować ręcznie. Połączenie *xrdp* nie wymaga tego wpisu i między innymi dlatego nie jest raczej polecane do dostępu z internetu.

Aplikacje administratora

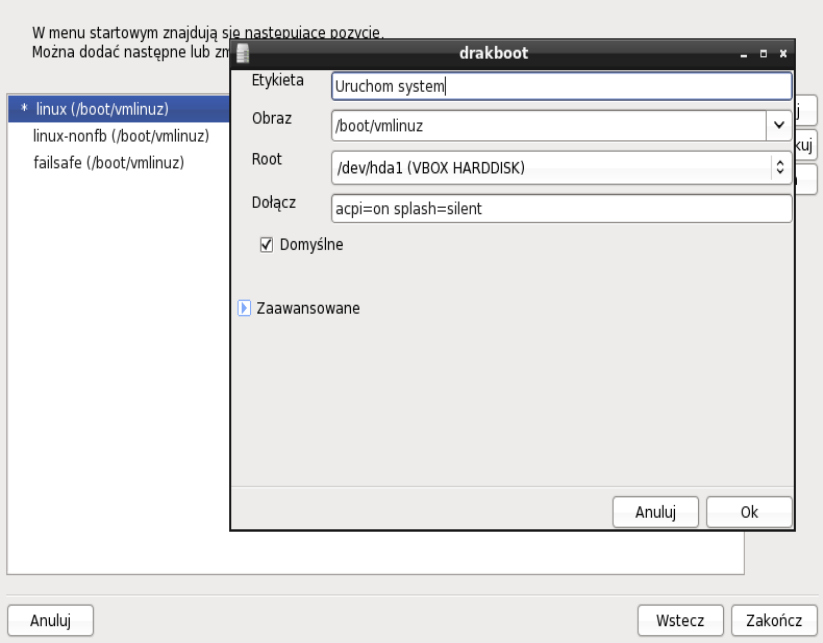
Trudno nawet w dość obszernym podręczniku omówić wszystkie możliwe aspekty działania systemu. Najważniejsze z nich zostały omówione w poprzednich rozdziałach. Dotyczą one przede wszystkim dostępnych na serwerze usług, a więc funkcji serwerowych i routerowych systemu. W bieżącym rozdziale znajdą się informacje o dodatkowych programach i konfiguracji, które mogą pomóc w bieżącej pracy.

Większość opcji dotyczących systemu, w tym konfigurację drukarki, wszystkie opcje sprzętowe, konfigurację sieci oraz działania usług konfigurujemy w czytelnym panelu administarcyjnym o nazwie *Konfiguracja komputera* (*Rysunek 80: Panel administracyjny systemu*). Panel jest szczególnie przydatny do skonfigurowania rozmaitych opcji sprzętowych, np do zmiany ustawień wyświetlania – rozdzielczości, głębi kolorów, czy sterowników karty graficznej. Nie należy go jednak używać do usług specjalnie skonfigurowanych w systemie EOS – dhcp, dns, samba, www, poczta, ftp, proxy i firewall. Do tych usług są przeznaczone osobne kreatory konfiguracji.



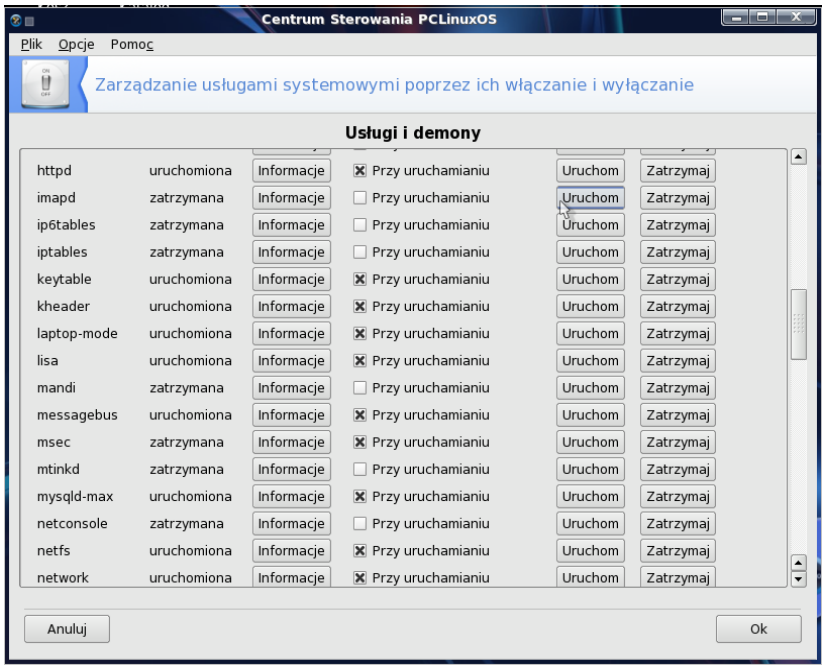
Rysunek 80: Panel administracyjny systemu

Podczas uruchamiania systemu pokazuje się menu wyboru, ma ono znaczenie głównie dla tych, którzy uruchamiają rożne systemy operacyjne na tym samym komputerze. Domyślnie po instalacji stacji lub serwera zobaczymy napis po angielsku. Można ustawić własną etykietę w *Konfiguracji komputera* w zakładce *Uruchamianie*, wybierając opcję *Konfiguracja sposobu uruchamiania*.



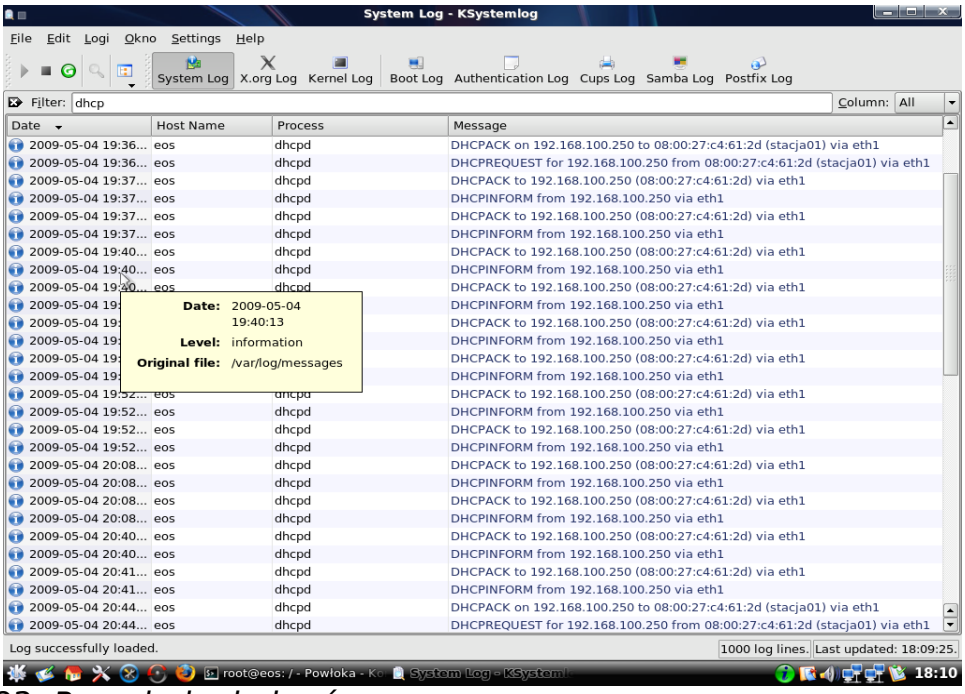
Rysunek 81: Zmiana etykiety systemu w bootloaderze

Usługi na serwerze można włączać i wyłączać, używając sekcji *System* panelu administracyjnego. System zawiera sporą grupę oprogramowania typowo serwerowego, lecz wiele opcji jest domyślnie wyłączonych, aby niepotrzebnie nie obciążały komputera, jeśli użytkownik ich nie potrzebuje.



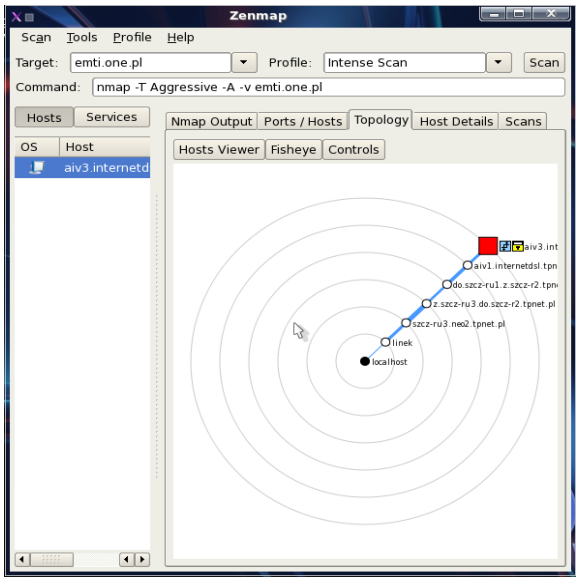
Rysunek 82: Okno zarządzania usługami w panelu administracyjnym

Do przeglądania logów można wykorzystać konsolę i program *mc*, ale jest też wygodna przeglądarka logów *Ksystemlog*, która wywołujemy z menu System – Monitorowanie (*Rysunek 83: Przeglądanie logów*). Ważną zaleta programu jest możliwość filtrowania wyświetlanych logów według grup usług, a także filtrowanie wyrażeń znajdujących sie w logach, dzięki czemu błyskawicznie można wyświetlić np. wszystkie wpisy dotycząc *dhcp*. Przeglądarka również zaznacza logi kolorami, a wiec łatwo zorientować się, które z nich zawierają zwykłe informacje, a które ostrzeżenia lub błędy.



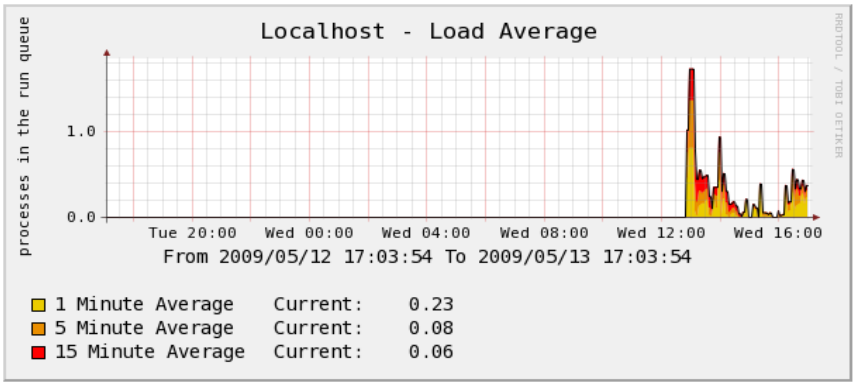
Rysunek 83: Przeglądanie logów

Przydatnym dla administratora narzędziem może być skaner *Nmap*. Pozwala on na skanowanie hostów w sieci wewnętrznej i na zewnątrz. Dzięki temu można sprawdzić np. dostępne porty, czy topologię połączenia. Warto jednocześnie ostrzec, że agresywne zachowanie programu, może zostać czasem odebrane jako próbę ataku, zatem lepiej być ostrożnym w skanowaniu obcych komputerów w internecie.



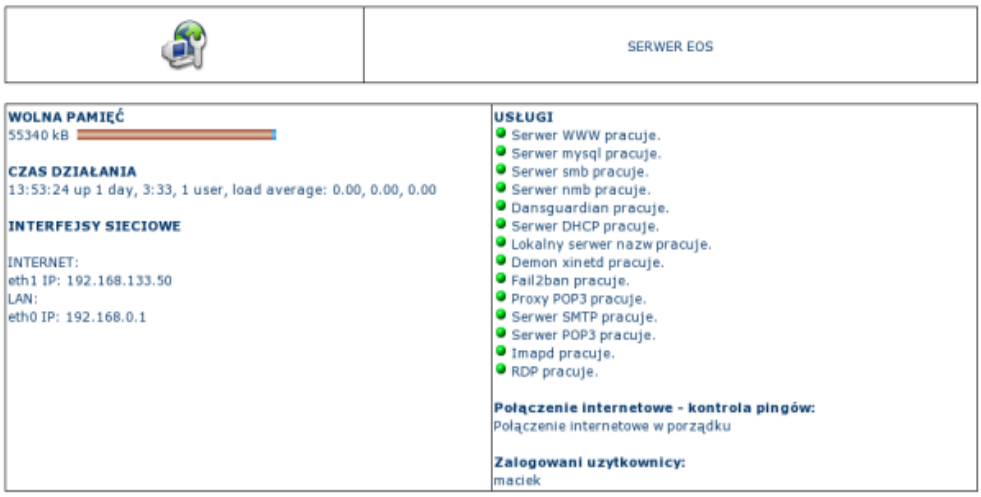
Rysunek 84: Okno programu nmap z graficzną nakładką

Większość administratorów pragnie mieć narzędzia, które pozwolą im monitorować stan systemu i najważniejsze parametry sieci. **EOS** zawiera sporą liczbę programów, które mogą być przydatne. Jednym z nich jest aplet pokazujący stan użycia dysku, innym *Strażnik systemu KDE*, ale najlepszym i najobszerniejszym narzędziem do monitorowania sieci i komputerów jest webowe narzędzie *Cacti* połączone z usługą *snmpd* i korzystające z *rrdtool*.



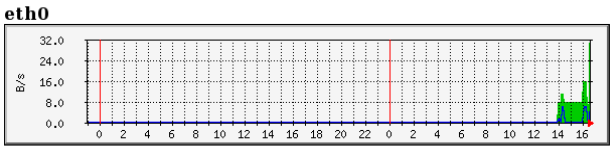
Rysunek 85: Wykresy Cacti

Cacti jest domyślnie zainstalowane i wywoływane z adresu *http://localhost/cacti* (*Rysunek 85: Wykresy Cacti*) – po pierwszym otwarciu strony należy się zalogować z domyślnym hasłem (admin:admin) i zmienić hasło. Potem trzeba skonfigurować program. Należy uruchomić usługę *snmpd* i dodać kolejne urządzenia w sieci, zdecydować o rodzaju tworzonych wykresów i uruchomić w cronie odpowiedni wpis dotyczący cacti, aby zacząć zliczać dane.



Rysunek 86: Strona wyświetlająca najważniejsze parametry serwera

Jeśli *Cacti* jest zbyt skomplikowanym narzędziem, każdy administrator ma domyślnie działająca stronę pod adresem *http://localhost/server.php* (Rysunek 86: Strona wyświetlająca najważniejsze parametry serwera) i może szybko zobaczyć najważniejsze parametry pracy serwera. Administrator ma też do dyspozycji podstawowe wykresy MRTG.

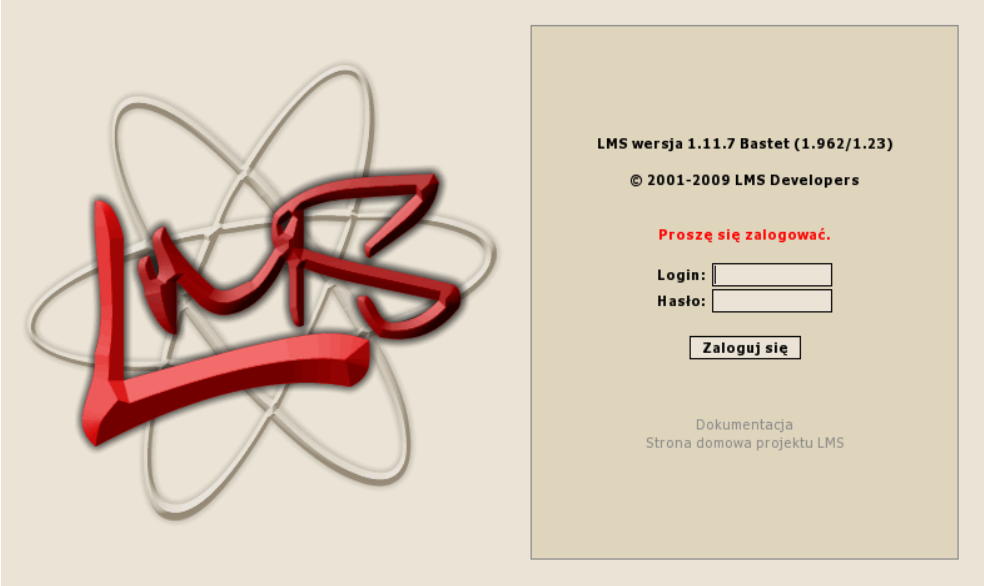


Rysunek 87: Przykład wykresu MRTG

Aby uruchomić rysowanie wykresów w skonfigurowanej postaci, należy tylko uaktywnić wykonywanie *mrtg* w cronie (*/var/spool/cron/root*). W przypadku chęci posiadania dokładnych danych np. o ruchu z każdego hosta, należy skonfigurować *mrtg* samodzielnie.

Dla administratorów sieci abonenckich, czyli takich, w których użytkownicy płacą za

dostęp do internetu, przydatnym narzędziem może być system LMS. Jest to również aplikacja webowa, która umożliwia zarządzanie siecią, w tym również stroną finansową przedsięwzięcia. System wymaga dość żmudnej konfiguracji i ręcznego dodawania wielu danych dotyczących użytkowników, ale stanowi nieocenioną pomoc w firmie (Rysunek 88: Okno logowania systemu LMS).



Rysunek 88: Okno logowania systemu LMS

Administratorzy, którym Cacti i LMS nie są potrzebne, nie muszą się obawiać, te systemy, jeśli nie pracują, nie używają zasobów systemowych, a katalogi */var/www/cacti* i */var/www/lms* domyślnie są widoczne tylko z localhosta. Aby je odblokować należy zmienić ustawienia w plikach, które zanajdują się w */etc/httpd/conf/webapps.d* – domyślnie jest w nich wpis *Deny from All* (trzeba zmienić na *Allow From All*). Każda z aplikacji ma swój własny plik konfiguracyjny.

Domyślnie nie jest włączony żaden mechanizm zarządzania przepływem pakietów na serwerze. W przypadku zastosowania systemu **EOS** w pracowni szkolnej i umiarkowanego korzystania z internetu pod kontrolą nauczyciela nie ma takiej potrzeby. Jednak limitowanie ruchu może być przydatne w razie swobodnego korzystania z internetu przez komputery klienckie. Służy do tego program *niceshaper*, który można uaktywnić w konfiguracji firewalla. Program należy skonfigurować edytując plik */etc/niceshaper/config* – najważniejsze są wpisy dotyczące interfejsów sieciowych w sekcji *<global>*, które należy dostosować do własnej konfiguracji:

iface inet eth0 auto
iface local eth1 192.168.100.1/24
oraz wpisy w sekcji *<download>* i *<upload>*, które są dostosowane do łącza ADSL o prędkości 1 Mbps.

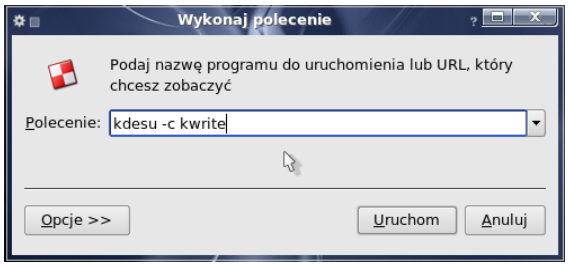
link speed 125kbps shape 110kbps
link speed 32kbps shape 25kbps

Niceshaper daje również możliwość zróżnicowania przypisanych prędkości w zależności od komputera klienckiego, należy wówczas wprowadzić odpowiednie wpisy w pliku */etc/niceshaper/users*. Możliwości *niceshapera* są dość rozbudowane, lecz wymagają od administratora wiedzy. Dokumentacja programu jest na stronie domowej: http://niceshaper.jedwabny.net i tam również znaleźć można przykłady tworzenia zaawansowanej konfiguracji. Dla zaawansowanych administratorów przeznaczony jest

konfigurator HTB, który dostępny jest pod adresem https://localhost/webhtb po zalogowaniu się hasłem roota (Rysunek 89: Logowanie do panelu WebHTB). Prawidłowe działanie WebHTB może wymagać ręcznej korekcji wartości wpisanych w bazie MySQL, a z całą pewnością wymaga zaawansowanej znajomości reguł HTB. Przed zastosowaniem programu warto zobaczyć najpierw http://webhtb.sourceforge.net/video_demo.html i poznnać zasady posługiwania się programem.

Rysunek 89: Logowanie do panelu WebHTB

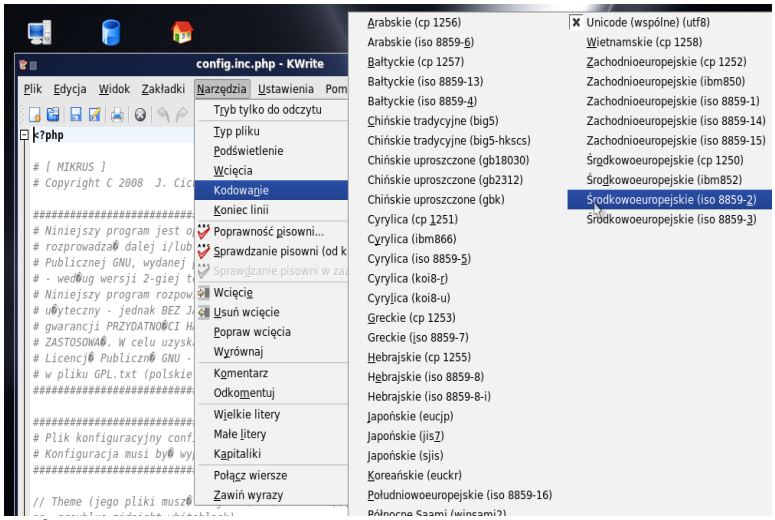
Edycja plików tekstowych może być istotnym elementem konfiguracji niektórych usług. Najprostszym sposobem jest użycie konsoli i programu *Midnight Commander*, jednak można edytować ważne pliki także używając okienkowego edytora *KWrite*. W przypadku tego ostatniego trzeba pamiętać, aby uruchamiać go na prawach roota inaczej



Rysunek 90: Uruchamianie aplikacji

nie będzie możliwe zapisanie plików systemowych. Wykonujemy to, wciskając klawisze ALT + F2 i wpisując *kdesu -c kwrite*. Ten sposób uruchamiania pozwala również na inne wywołania programów z prawami roota w podobny sposób. Nie jest potrzebne podawanie ścieżki do programu, a wyłącznie wpisanie nazwy (Rysunek 90: Uruchamianie aplikacji).

Jeśli chcemy edytować pliki stron *html*, które domyślnie znajdują się w */var/www*, warto pamiętać o prawidłowym kodowaniu. **EOS** używa kodowania *UTF-8* zarówno w aplikacjach okienkowych, jak i konsolowych, ale część stron internetowych nadal stosuje kodowanie *ISO-8859-2* i trzeba o tym pamiętać, edytując strony. W edytorze *KWrite* mamy ogromny wybór dostępnych opcji kodowania (Rysunek 91: Wybór kodowania).

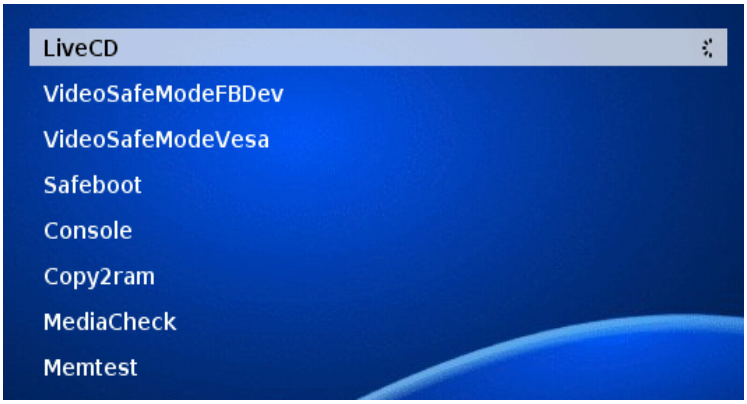


Rysunek 91: Wybór kodowania

Rozwiązywanie problemów

1. Błędy uruchamiania wersji *Live*

System powinien sie uruchamiać w trybie graficznym, aż do momentu pojawienia się graficznego okna logowania. Jeśli tak się nie dzieje, mogą być dwie możliwe przyczyny – problemy z wyświetlaniem lub z odczytem płyty.



Rysunek 92: Menu startowe płyty

W przypadku kłopotów z kartą graficzną można zastosować kilka rozwiązań. Po pierwsze podczas uruchamiania można wybrać opcję *VideoSafeModeFBDev* lub *VideoSafeModeVesa* (*Rysunek 92: Menu startowe płyty*). Szczególnie ta druga opcja zapewnia nam graficzne uruchomienie systemu, jeśli tylko karta graficzna zgodna jest ze standardem *VESA*. Jeśli system nie uruchamia się graficznie, można zalogować się w trybie tekstowym i wpisać polecenie *startx*. W takim przypadku zobaczymy ekran graficzny lub komunikaty o błędach. Niektóre karty *Nvidia* wbudowane na płytach powodują, że system nie uruchamia się graficznie ponieważ nie potrafią automatycznie zmienić parametrów po wstępnym etapie uruchamiania. Ręczne uruchamianie systemu graficznego udaje się. Należy wówczas wybrać w konfiguracji mniej „wyśrubowane” ustawienia lub zastosować sterownik vesa. Należy pamiętać, że zawsze można spróbować konfiguracji graficznej i wybrania odpowiedniejszych sterowników oraz parametrów wyświetlania.

Gorsza sytuacja następuje wówczas, gdy po krótkiej procedurze wstępnej pojawia nam się tzw. ograniczony shell. Oznacza to zwykle i taki też jest komunikat na ekranie, że system nie mógł wczytać pliku *livecd.sqfs*. Niestety zwykle to kończy próby uruchomienia systemu z takiej płyty i wymaga wykonania następnej. Przyczyną bywa zły stan czytnika lub nagrywarki, a także zbyt duża szybkość nagrywania płyty, co współcześnie jest dość częstym problemem – zbyt duża prędkość zapisu powoduje, że inne czytniki mają problem z taką płytą.

O dokumencie

Niniejszy dokument zawiera opis instalacji, konfiguracji oraz pracy na serwerze oraz stacji roboczej **EOS**. Informacje na temat działających na serwerze usług są ograniczone do niezbędnych wskazówek konfiguracyjnych i z pewnością nie wyczerpują tematu, z tego względu użytkownik zainteresowany wdrożeniem innych niż podstawowe funkcji, powinien szukać bardziej obszernych informacji.

Dokument niniejszy jest udostępniany „w stanie, w jakim się znajduje” z nadzieją przydatności, ale bez jakiejkolwiek gwarancji wyraźnej lub dorozumianej, w tym bez gwarancji przydatności handlowej lub przydatności do określonego celu. Właściciel praw autorskich określony w niniejszej informacji o uprawnieniach nie jest w żadnym wypadku odpowiedzialny za jakiekolwiek roszczenia, ani za jakiekolwiek szkody szczególne, pośrednie lub wtórne, ani żadne inne szkody wynikające z zastosowania się do wskazań niniejszego dokumentu..

Licencja:
Creative Commons BY-NC-SA 3.0
Szczegółowe warunki oraz pełny tekst licencji można znaleźć pod adresem:
http://creativecommons.org/licenses/by-nc-sa/3.0/deed.pl

Wiesław M. Trąmpczyński