

PPP w Linuksie

Autor: [Wojciech Zakroczymski](#)

Coraz większa liczba serwerów podłączanych do Internetu wykorzystuje system Linux. Przemawiają za tym przede wszystkim względy ekonomiczne - system jest dostępny za darmo i ma skromne wymagania sprzętowe. W tym artykule oprócz sporej dawki teorii omawiamy kwestie związane z serwerem PPP, natomiast na str. XX-XX prezentujemy trochę inne podejście do tego samego tematu - sposób podłączenia sieci lokalnej do Internetu ze szczegółowym opisem kompilacji jądra Linuksa i możliwości zestawiania połączenia na żądanie.

W wielu sieciach teleinformatycznych konieczne jest czasem stworzenie łącza stałego typu punkt-punkt, np. przy łączeniu dwóch sieci wewnątrz firmy. Przy podłączaniu firmy do Internetu zarówno łączem komutowanym, jak i stałym, też mamy do czynienia z połączeniem typu punkt-punkt. W celu zapewnienia jednolitego sposobu komunikacji został stworzony protokół transmisji danych dla takich łączy - PPP (Point to Point Protocol). Jego działanie polega na przenoszeniu pakietów protokołów wyższych warstw - IPX, DECNET czy wreszcie najważniejszego dla Internetu IP - przez łącze punkt-punkt.

Oprogramowanie

Źródła jądra systemu Linux są dostępne w Internecie. Pod adresem: www.kernel.org jest nawet specjalna strona zawierająca najnowsze stabilne i rozwojowe wersje systemu. Również z każdą dystrybucją systemu rozprowadzane są źródła jądra w postaci pakietów.

Po ściągnięciu z Internetu źródeł systemu (najczęściej w pliku `kernel-source*.tar.gz`) należy plik ten skopiować do katalogu `/usr/src/linux` i jako root wydać komendę: `tar -vzxvf kernel-source*.tar.gz`. Spowoduje to rozpakowanie archiwum i właściwe zainstalowanie źródeł systemu.

Aby móc używać protokołu PPP, konieczne jest odpowiednie skompilowanie jądra systemu Linux, tak aby zawierało obsługę tego protokołu, oraz zainstalowanie oprogramowania demona `pppd`. Oprogramowanie to znajduje się w każdej dystrybucji systemu Linux, trzeba tylko pamiętać o zaznaczeniu właściwej opcji podczas instalacji. Należy również zainstalować źródła jądra systemu (kernel source) - można to zrobić od razu lub ściągnąć je później z Internetu (patrz ramka 1).

Kompilacja jądra

Linux jest rozprowadzany na licencji GNU, a więc wraz z kodem źródłowym. Użytkownik może więc konfigurować jądro systemu stosownie do własnych potrzeb. Mechanizm konfiguracji i kompilacji jądra jest dość prosty. Należy zalogować się do systemu jako root i przenieść się do katalogu `/usr/src/linux`, a następnie wydać komendę `make config` i przystąpić do konfigurowania opcji kompilacji systemu. W tym momencie trzeba wybrać cały szereg opcji konfiguracyjnych, począwszy od sterowników dysków, poprzez systemy plików, na sterownikach kart dźwiękowych skończywszy. Oczywiście wybór ten będzie zależał od parametrów posiadanego sprzętu oraz od tego, jakie zadania system będzie wykonywał.

Do obsługi protokołu PPP konieczne jest zaznaczenie odpowiedniej opcji:

```
PPP (point-to-point) support (CONFIG_PPP) [y/n]
```

a także opcji tunelowania protokołu IP (IP tunneling). Warto również wybrać obsługę firewalli (IP firewalling) - sieć firmowa podłączona do Internetu jest narażona na włamania z Sieci, trzeba więc zadbać o jej ochronę.

Ponieważ jądro systemu znajduje się cały czas w pamięci operacyjnej i nie może być zapisywane na dysku, dąży się do zmniejszenia jego wielkości przez wprowadzenie modułów. Moduł jest to część jądra, która może być w dowolnym momencie umieszczona w pamięci (gdy jest potrzebna) oraz usunięta z niej. Obsługę PPP również można skompilować jako moduł. W tym celu w pierwszej fazie konfiguracji należy włączyć obsługę modułów:

```
Enable loadable module support (CONF_MODULES) [y/n/?]
```

a następnie na pytanie o PPP

```
PPP (point-to-point) support (CONF_PPP) [M/n/y/?]
```

odpowiedzieć M, tzn. wybrać kompilację jako moduł.

Kolejne kroki kompilacji systemu to polecenia: `make dep`, następnie `make zImage` i na końcu `make zilo` - instalacja nowego jądra. Przy instalacji jądra z modułami konieczne jest jeszcze, po przeładowaniu systemu, wydanie komendy `make modules` oraz zainstalowanie modułów poleceniem `make modules_install`. Szczegółowe informacje na temat kompilacji jądra i poszczególnych opcji konfiguracyjnych można znaleźć w Kernel-HOWTO, dokumencie rozprowadzanym wraz z dystrybucją systemu.

Porty szeregowy i modem

Do łączenia dwóch sieci konieczne jest zastosowanie odpowiednich modemów na linie dzierżawione. Do ich prawidłowego działania konieczne jest właściwe skonfigurowanie portów szeregowych. Często dwa porty szeregowy działają na jednym przerwaniu. W takiej sytuacji należy przestawić przerwań (wiele nowych kart wejścia-wyjścia na to pozwala). W przypadku niestandardowego ustawienia przerwań na portach szeregowych należy powiadomić o tym system operacyjny za pomocą programu `setserial` (np. `/bin/setserial -b /dev/ttyS2 IRQ 11`, gdzie `ttyS2` - COM3 pod DOS). Problem z przerwaniami może się pojawić tylko przy korzystaniu z więcej niż dwóch portów szeregowych (kilka połączeń PPP z jednego komputera), ponieważ właśnie trzeci i czwarty port dzielą wspólne przerwanie.

Przy podłączaniu sieci do Internetu z reguły to dostawca zajmuje się stroną sprzętową - wynajmuje klientowi modemy oraz zestawia połączenie - i użytkownik nie musi sam wprowadzać żadnych zmian. Jeśli jednak instalujemy własne urządzenia, należy zwrócić uwagę na ustawioną szybkość modemu oraz na sposób kontroli przepływu danych. Zalecane jest używanie sygnałów sprzętowych (CTS/RTS) z uwagi na możliwość pojawienia się w sygnale sekwencji kontrolnych, co może powodować problemy.

Adresy IP

Istnieją trzy główne klasy numerów IP:

- Numery klasy A - zawierają sieci od numeru 1.0.0.0 do 127.0.0.0. W adresie takim pierwszy oktet (osiem bitów) to numer sieci. Daje to 24 bity na adres hosta, tzn. sieci te mogą zawierać do 1,6 miliona komputerów.
- Numery klasy B - zawierają sieci od numeru 128.0.0.0 do 191.255.0.0. Tutaj numer sieci to pierwsze dwa oktety. Pozwala to na zaadresowanie 16 320 sieci, z których każda może liczyć po 65 024 komputery.
- Numery klasy C - zawierają sieci od numeru 192.0.0.0 do 223.225.225.0. Adres sieci to trzy pierwsze oktety, co oznacza, że sieć taka zawiera do 254 komputerów.

Występują też numery IP przeznaczone specjalnie dla sieci, które nie są podłączone do Internetu. Nie można pod żadnym pozorem wykorzystywać tych adresów w Internecie. Są to:

- jeden numer klasy A - 10.0.0.0 (maska podsieci 255.0.0.0),
- 16 numerów klasy B - od 172.16.0.0 do 172.31.0.0 (maska podsieci 255.255.0.0),
- 256 numerów klasy C - od 192.168.0.0 do 192.168.255.0 (maska podsieci 255.255.255.0).

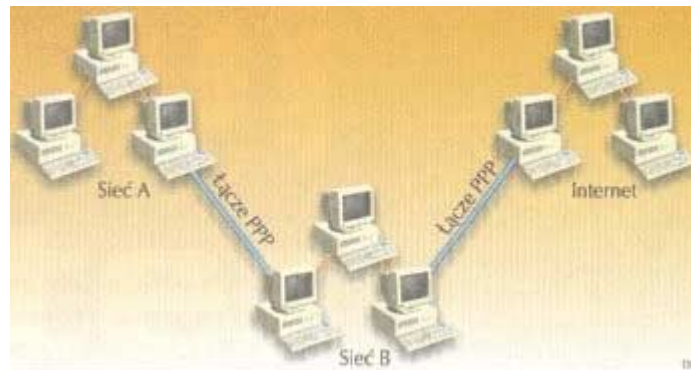
Obowiązkiem dostawcy Internetu jest, oprócz zestawienia połączenia dzierżawionego, dostarczenie puli adresów IP dla podłączanej do Internetu sieci oraz zapewnienie zapasowego serwera DNS poza łączem PPP. W przypadku łączenia dwóch sieci lokalnych należy samodzielnie wybrać adres z zakresu adresów nie wykorzystywanych w Internecie (patrz ramka 2).

Demon pppd

Do prawidłowego działania protokołu PPP konieczna jest odpowiednia konfiguracja opcji jego działania. Standardowo zainstalowany pakiet `ppp` tworzy kilka plików na dysku, ulokowanych w podkatalogu `ppp` katalogu `/etc`. Są to pliki:

- `/etc/ppp/options` - główny plik konfiguracyjny,
- `/etc/ppp/options.ttyXX` - pliki konfiguracyjne dla poszczególnych portów szeregowych,

- /etc/ppp/ip-up - plik wykonywany po uruchomieniu interfejsu ppp.



Zastosowanie łączy punkt-punkt do stworzenia sieci WAN

Opcje identyczne dla wszystkich interfejsów ppp dla danego komputera umieszczamy w pliku options, zaś specyficzne dla danego łącza (jak na przykład numery IP) - w plikach options.ttyXX. Do podstawowych opcji, koniecznych do zaznaczenia w przypadku łącza stałego należą:

- -detach - zabezpiecza przed wykonywaniem procesu w tle,
- modem - włącza korzystanie z linii kontrolnych modemu,
- lock - włącza blokowanie portu szeregowego,
- crtscts - zapewnia sprzętową kontrolę przepływu danych,
- defaultroute - ustawia w tablicy routingu domyślną drogę na interfejs ppp (opcję tą należy wykorzystywać jedynie przy połączeniu z Internetem),
- asynmap 0 - nie ustawia żadnych kontrolnych sekwencji wyjściowych.

Pozostałe opcje można pozostawić bez zmian. Wartości przyjmowane domyślnie są zadowalające. Oczywiście należy również podać w plikach konfiguracyjnych adresy IP po obu stronach łącza ppp. Podaje się je w formie LOCAL_IP:REMOTE_IP, gdzie LOCAL_IP jest przyznanym przez dostawcę Internetu (lub wybranym z puli adresów nie używanych) adresem IP komputera, na którym uruchamiamy demona pppd, natomiast REMOTE_IP jest numerem komputera po drugiej stronie łącza ppp.



Routing w sieci wykorzystującej łącza PPP

Po takim przygotowaniu plików konfiguracyjnych pozostaje tylko uruchomić program demona. Służy do tego polecenie

```
pppd -d /dev/ttySx 115200 &
```

Opcja -d włącza śledzenie działania protokołu, co pozwala znaleźć ewentualne błędy jego uruchomienia (wszelkie komunikaty zapisywane są do logu systemowego). Zapis /dev/ttySx to oczywiście port, do którego podłączony

jest modem (ttyS0 - COM1, ttyS1 - COM2 itd.). Ostatni parametr to szybkość wysyłania danych na port. Oczywiście wszelkie opcje podawane przy uruchomieniu protokołu można umieścić w plikach konfiguracyjnych.

Po uruchomieniu programu pppd powinny zapalić się diody modemu, co oznacza przesłanie danych na drugą stronę łącza i uzgodnienie opcji konfiguracyjnych protokołu. Od tej pory łącze stałe powinno działać, co można sprawdzić na przykład za pomocą komendy ping xxx.xxx.xxx.xxx, podając adres IP spoza łącza. W razie braku odpowiedzi należy sprawdzić log systemowy i zobaczyć, gdzie nastąpił błąd podczas uruchamiania pppd. Można też użyć komendy ifconfig, która wyświetla aktywne interfejsy sieciowe. Jeśli nie pokazuje się interfejs pppx, gdzie x to numer interfejsu, oznacza to, że nastąpił błąd podczas uruchamiania pppd. W przeciwnym wypadku należy sprawdzić wyświetlane przez tę komendę dane o interfejsie (takie jak adresy IP). Prawdopodobnie błąd tkwi w routingu (na przykład brak opcji defaultroute).

Teraz należy umieścić komendę pppd w którymś z plików startowych. W zależności od dystrybucji systemu są to:

- dla Slackware (pliki startowe BSD): /etc/rc, /etc/rc.local oraz /etc/rc.serial
- dla Debian i RedHat (pliki startowe System V): /etc/rc.d/rc, /etc/rc.d/rc.local, /etc/rc.d/rc.sysinit oraz pliki w katalogach /etc/rc.d/rc0.d, /etc/rc.d/rc1.d ... /etc/rc.d/rc6.d.

Routing

W podkatalogu ppp znajduje się [plik ip-up](#). Jest to skrypt uruchamiany po wystartowaniu interfejsu ppp. Można więc w nim umieścić polecenia wykonania wszelkich koniecznych czynności po uruchomieniu połączenia. Szczególnie ważne jest odpowiednie ustawienie routingu między łączonymi sieciami. Mamy tu dwie możliwości. W pierwszym przypadku, gdy łącze stałe jest łączem do Internetu, domyślna droga pakietów powinna prowadzić właśnie przez interfejs ppp. Drogę tę ustawia opcja defaultroute programu pppd. Przy łączeniu dwóch sieci LAN konieczne jest ustawienie drogi dla adresów odpowiedniej podsieci.

Do wprowadzania zmian w tablicy routingu służy komenda route. Za jej pomocą można ustawiać drogę dla pakietów kierowanych do konkretnej podsieci (route add net) oraz drogę dla konkretnego adresu IP (route add host). Można też dodać domyślną drogę pakietów (route add default), a także usunąć drogę pakietów z tablicy routingu jądra systemu.

W pliku ip-up można też umieścić polecenia wykonania innych czynności, na przykład wysyłanie zaległej poczty, czyszczenie niepotrzebnych plików. Należy jedynie pamiętać, że ten sam plik jest uruchamiany dla każdego portu szeregowego, więc trzeba umieścić osobny fragment dla każdego z nich i rozróżniać, z którym portem mamy do czynienia. Przydaje się do tego, jak widać na przykładzie, komenda powłoki case.

Jak już wspominałem, dobrze jest zapoznać się z oprogramowaniem ipfadm, w celu lepszej ochrony sieci wewnętrznej przed włamaniem z Internetu. Oprogramowanie to pozwala na filtrację przychodzących pakietów i kontrolę dostępu do sieci z zewnątrz. Pozwala też na podłączenie do Internetu całej sieci firmowej, nawet jeśli mamy tylko jeden numer IP, poprzez zastosowanie tzw. maskarady, czyli maskowania adresów sieci wewnętrznej.

Serwer PPP

Stworzenie serwera PPP, czyli przyjmowanie połączeń z zewnątrz jest bardzo proste. Przede wszystkim należy ustawić modem na odbieranie połączeń (według jego instrukcji obsługi). Następnie należy tak ustawić serwer, aby zgłaszał terminal na porcie szeregowym. W tym celu, w pliku /etc/inittab należy dodać linię:

```
Sx:12345:respawn:/sbin/uucpgetty -h -t120 ttySx 115200 vt100
```

gdzie x - numer portu.

Po ustaleniu protokołu przez modemy użytkownik dzwoniący do serwera otrzyma terminal, na którym powinien uruchomić demona pppd. Niestety, do manipulacji interfejsem sieciowym konieczne są uprawnienia superużytkownika. Należy więc odpowiednio ustawić uprawnienia do pliku /sbin/pppd, czyli demona ppp. Plik ten powinien mieć atrybut użytkownika przy wykonaniu (tzw. SETUID). Ponieważ należy on do użytkownika root, będzie wykonywał się na jego prawach. Aby wybrać niezbędne ustawienia, trzeba jako użytkownik root przejść do katalogu /sbin i wydać polecenie

```
chmod u+s pppd
```

Warto również napisać prosty skrypt uruchamiający demona pppd o nazwie np. ppp. Skrypt taki oprócz dynamicznego przydzielania numeru IP z puli dostarczonej przez dostawcę Internetu mógłby sprawdzać również,

z którego portu loguje się użytkownik (jeśli są co najmniej dwa modemy) i czy ma do tego prawo.

Do przyjmowania połączeń konieczne jest wkompilowanie w jądro, oprócz wymienionych wyżej opcji, również opcji IP forwarding. Routing w tym przypadku obsługiwany jest przez użycie parametru proxyarp demona pppd. Parametr ten dodaje wpis w tablicy ARP serwera ppp, co powoduje właściwe routowanie pakietów do klienta ppp. Przykładowy skrypt ppp znajduje się [tutaj](#).

Informacje dodatkowe

na temat obsługi protokołu PPP przez system Linux można znaleźć przede wszystkim w dokumentach HOWTO rozprawdzanych razem z systemem:

- opis PPP - w dokumencie PPP-HOWTO,
- dokładny opis konfigurowania i użytkowania portów szeregowych pod Linuksem - w Serial-HOWTO,
- sposób kompilacji jądra - w Kernel-HOWTO.

Zajrzyj

www.linuxdoc.org/LDP - strony Linux Documentation Project (zawierają m.in. doskonały przewodnik po zagadnieniach sieciowych w systemie Linux, czyli The Network Administrator's Guide),

www.linux.org - strona Linux User's Group,