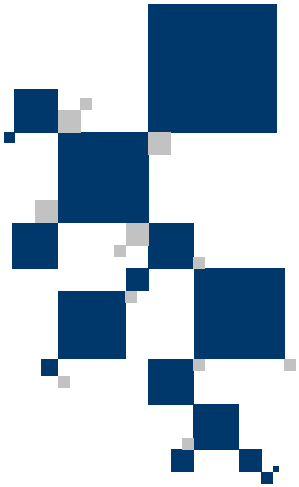

INSTRUKCJA UŻYTKOWNIKA

Routery V.35 / Ethernet serii

TAHOE 1800

TAHOE

WOLNOŚĆ KOMUNIKACJI

SPIS TREŚCI

Tahoe® 1801 (V.35 / 10Base-T)
Tahoe® 1808 (V.35 / switch 10/100Base-T)

Instrukcja użytkownika

http://www.tahoe.pl/

Oprogramowanie systemowe wersja 1.2.5

1. Wprowadzenie

Routery serii Tahoe® 1800 występują obecnie w dwóch wersjach:

- **Tahoe® 1801** posiada jeden port szeregowy **V.35** oraz jeden port Ethernet 10Base-T.

- **Tahoe® 1808** również posiada port **V.35**, ale zamiast pojedynczego portu Ethernet 10Base-T posiada wbudowany **8-portowy zarządzalny przełącznik 10/100Base-T**.

Routery znakomicie współpracują z sieciami opartymi na protokołach Frame Relay, synchronicznym PPP lub Cisco® HDLC.

Oprogramowanie routera obsługuje protokoły IP, ARP, TCP, UDP, ICMP. Jest możliwe zarządzanie nim przez telnet, przez SNMP oraz przez port konsoli szeregowej. Statystyki pracy są dostępne przez WWW. Przebieg pracy routera może być przesyłany przy pomocy protokołu syslog do centralnego serwera.

Jeden interfejs sieciowy może obsłużyć kilka podsieci IP poprzez aliasy interfejsów (eth0:0, eth0:1, itd.) oraz interfejsy VLAN (eth0.1, eth0.2, itd.). Router może również pracować jako bridge pomiędzy dwiema podsieciami, dzięki czemu dwie sieci LAN połączone przez sieć Frame Relay lub inną sieć rozległą tworzą jedną całość na poziomie sprzętowym (np. komputery z systemem Microsoft® Windows™ widzą się w otoczeniu sieciowym).

Dostępny jest serwer DHCP/BOOTP umożliwiający przydzielenie komputerom w sieci adresów IP, masek podsieci, adresów routerów i serwerów DNS i wielu innych parametrów niezbędnych do pracy. Oprócz serwera DHCP w routerze jest DHCP/BOOTP Relay Agent przekazujący zapytania DHCP/BOOTP z danej podsieci do innego serwera.

Router obsługuje maskaradę (NAT), tj. umożliwia dostęp do internetu całej podsieci przy wykorzystaniu tylko jednego adresu IP. Ponadto jest możliwa filtracja ruchu (firewall) na podstawie adresów IP, portów TCP i UDP oraz protokołów pojawiających się w przesyłanych pakietach.

Oprogramowanie systemowe (firmware) jest zapisane w pamięci Flash - można je aktualizować przy użyciu TFTP. Ustawienia są przechowywane w pamięci EEPROM.

2. Interfejs Ethernet

Interfejs Ethernet służy do podłączenia routera do sieci LAN. Powinien on być podłączony zwykłym patch-cordem do zwykłego portu koncentratora lub przełącznika, a skrosowanym do komputera, innego routera albo portu „uplink" w koncentratorze lub przełączniku. Po podłączeniu w interfejsie zapali się dioda „LINK".

W przypadku wersji z wbudowanym przełącznikiem nie trzeba zwracać uwagi na typ patch-corda, ponieważ przełącznik automatycznie rozpoznaje, czy kabel jest skrosowany, czy nie.

W routerze **Tahoe® 1801** interfejs Ethernet posiada następujące diody LED:

- **LNK -** połączenie z siecią LAN (Link)
- **COL** - kolizja w sieci LAN (Collision)
- **LRX** - odbiór z sieci LAN (LAN Receive)
- **LTX** - nadawanie do sieci LAN (LAN Transmit)

W routerze **Tahoe® 1808** stan każdego z portów wbudowanego przełącznika jest sygnalizowany następującymi diodami LED:

- **10/100 Mbps -** zapalona oznacza połączenie 100 Mb/s
- **LINK/ACTIVITY -** zapalona oznacza, że jest połączenie z siecią LAN, miga w momencie przesyłania danych
- **DUPLEX/COLLISION -** zapalona na stałe oznacza połączenie Full-duplex, migająca - kolizje w połączeniu Half-duplex

Standardowo router jest dostarczany z ustawionym na interfejsie Ethernet adresem IP 10.0.0.1 i maską podsieci 255.0.0.0 i hasłem dostępu „**Tahoe**".

3

3. Konfiguracja przez telnet lub konsolę szeregową

3.1

3. 1. Połączenie z routerem przez telnet

Aby móc się połączyć z zupełnie nieskonfigurowanym routerem należy tak skonfigurować interfejs sieciowy w komputerze, aby znajdował się w tej samej podsieci, co router. Standardowo router ma ustawiony adres IP 10.0.0.1 i maskę podsieci 255.0.0.0. Komputer, z którego router będzie konfigurowany może mieć adres np. 10.0.0.2 i maskę również 255.0.0.0.

Jeśli router był już wcześniej konfigurowany i ma poprawnie ustawiony routing, to można się z nim połączyć z dowolnego miejsca sieci podając jego adres IP.

Po połączeniu pojawia się pytanie o hasło dostępu:

```
User Access Verification

Password:
```

Standardowe hasło to „**Tahoe**" , a użytkownik to „**root**" (bez cudzysłowów, są rozróżniane duże i małe litery). Jeśli wpisane hasło jest poprawne, pojawia się linia komend:

```
Tahoe>
```

3.2

3.2. Połączenie przez konsolę szeregową

W przypadku braku możliwości połączenia przez telnet (np. brak odpowiednich narzędzi lub nieznajomość adresu IP routera) przy pomocy kabla null-modem można podłączyć router do portu szeregowego w komputerze. Router posiada złącze DB9 męskie o następujących wyprowadzeniach:

Pin	Sygnał	Opis
2	RxD	Dane odbierane
3	TxD	Dane nadawane
5	GND	Masa

W przypadku łączenia do złącza DB9 lub DB25 w komputerze,

piny należy połączyć według jednego z następujących schematów:

Pin w routerze (DB9)	Pin w PC (DB9)
2	3
3	2
5	5

Pin w routerze (DB9)	Pin w PC (DB25)
2	2
3	3
5	7

Kontrola przepływu w PC powinna być wyłączona. Ustawienia portu: 9600 b/s, 8N1

3.3. Polecenia 3.3

3.3.1. ?, help 3.3.1

Wpisanie „?" lub „help" wypisuje listę dostępnych poleceń.

3.3.2. arp 3.3.2

Polecenie „arp" służy do konfiguracji tablicy ARP. Samo „arp" wyświetla tablicę powiązań między adresami IP a adresami sprzętowymi (MAC):

```
Tahoe> arp
Adres IP       Adres sprzętowy
10.0.0.2     00:50:04:0D:70:31    dynamiczny
```

Wpisy w tablicy ARP można usunąć wpisując:

```
Tahoe> arp del 10.0.0.2
```

(gdzie zamiast „10.0.0.2" powinien się znaleźć adres IP, którego wpis chcemy usunąć).

Można dodać statyczny wpis ARP przy użyciu „arp add":

```
Tahoe> arp add 10.0.0.3 00:50:13:E9:5C:01
```

Przy pomocy polecenia „ifconfig" można włączyć lub wyłączyć

dynamiczne powiązanie adresów IP z adresami sprzętowymi. Jeśli powiązanie dynamiczne dla danego interfejsu będzie wyłączone, wówczas będzie możliwe nawiązanie połączenia tylko z tymi stacjami, których adres sprzętowy będzie statycznie wpisany przy pomocy „arp add". W ten sposób można zabezpieczyć sieć przed niepowołanym dostępem.

3.3.3

3.3.3. bridge

Komenda „bridge" włącza lub wyłącza tryb bridge. Włączenie tego trybu powoduje, że router staje się przezroczysty dla wszystkich rodzajów pakietów. Dwie sieci LAN podłączone do routerów (pomiędzy którymi jest sieć rozległa, np. Frame Relay) zachowują się tak, jakby były połączone bezpośrenio skrętką - komputery po obydwu stronach należą do tej samej podsieci IP. Jeśli pracują pod kontrolą systemu operacyjnego Microsoft® Windows™ to widzą się w otoczeniu sieciowym.

Są dostępne trzy tryby pracy:

- **off** - normalny routing tcp/ip pomiędzy interfejsami
- **on** - bridge włączony, ale router jest wciąż dostępny pod swoimi adresami IP, tak więc można nim zarządzać przez telnet lub SNMP
- **transparent** - zupełnie przezroczysty bridge - po włączeniu tego trybu router przestaje odpowiadać pod swoim adresem IP, tak więc wyłączenie tego trybu jest możliwe wyłącznie przez konsolę szeregową

Wpisanie **„bridge list"** wyświetla pamiętane adresy sprzętowe (MAC) wraz z informacją, po której stronie łącza pojawił się dany adres

Uwaga! Aby bridging działał poprawnie należy wskazać, pomiędzy którymi interfejsami ma być dokonywany. Służy do tego komenda „ifconfig <nazwa interfejsu> bridge on" - należy jej użyć dla każdego interfejsu, który ma być brany pod uwagę.

3.3.4

3.3.4. console

Komenda służy do włączenia lub wyłączenia kontroli dostępu przez konsolę. Standardowo użytkownik po podłączeniu do konsoli ma bezpośredni dostęp do linii komend. Po wpisaniu:

```
console passwd on
```

router będzie wymagał zalogowania, tak jak przy połączeniu przez

telnet. Aby wyłączyć kontrolę dostępu należy wpisać:

```
console passwd off
```

3.3.5. dhcp

3.3.5

Polecenie „dhcp" służy do konfiguracji serwera DHCP/BOOTP oraz DHCP/BOOTP Relay Agenta.

Serwer DHCP/BOOTP umożliwia przydzielanie adresów IP, masek podsieci, nazw domen, adresów serwerów DNS i innych parametrów komputerom w danej podsieci. Sieć, w której komputery pobierają dane z serwera DHCP lub BOOTP jest łatwo przekonfigurować - wystarczy zmienić ustawienia na serwerze, a wszystkie stacje automatycznie się dostosują.

Protokół BOOTP jest prostszą odmianą DHCP. Częstym jego zastosowaniem jest bootowanie komputerów bezdyskowych - protokół przekazuje klientowi adres IP, maskę podsieci, bramkę, nazwę pliku z systemem operacyjnym oraz adres serwera TFTP, z którego można ten plik ściągnąć.

Protokół DHCP pozwala na przekazanie wielu innych ustawień, takich jak nazwa domeny, adres serwera DNS, serwera drukarek, serwera logującego (syslog), fontservera dla X-Window, ustawień MTU i default TTL i innych.

DHCP/BOOTP Relay Agent służy do przekazywania zapytań DHCP i BOOTP pomiędzy sieciami. Standardowo protokoły DHCP i BOOTP działają w obrębie jednej fizycznej podsieci. Relay Agent wyłapuje zapytania z podsieci, do której jest podłączony i przekazuje je do serwera DHCP, który może znajdować się w dowolnym miejscu sieci.

3.3.5.1. Przeglądanie ustawień

3.3.5.1

Wpisanie samego „dhcp" wyświetla bieżące ustawienia - oto przykład konfiguracji serwera:

```
Tahoe> dhcp
DHCP/BOOTP server
default-lease-time 43200
max-lease-time 86400
network "lan" (eth0):
    default-lease-time 43200
    max-lease-time 86400
```

```
        domain-name tahoe.pl
        subnet "local": 10.0.0.0/255.255.255.0
            default-lease-time 43200
            max-lease-time 86400
            filename vmlinuz.2.2.19
            next-server 192.168.0.5
        routers 10.0.0.1
            domain-name-servers 192.168.0.4
            domain-name tahoe.pl
            address ranges: 10.0.0.3-10.0.0.15
    relay server 192.168.0.5 67
```

3.3.5.2

3.3.5.2. Ogólne zasady konfiguracji serwera DHCP / BOOTP

Przed przystąpieniem do konfiguracji serwera DHCP/BOOTP należy zapoznać się z poniższymi wskazówkami:

- konfiguracja ma strukturę hierarchiczną - najbardziej ogólną grupą jest „network" - fizyczna sieć podłączona do routera. W obrębie sieci może występować dowolna ilość podsieci IP. Z każdej podsieci IP może być wydzielony jeden lub kilka zakresów adresów IP, które mogą być dynamicznie przydzielane komputerom. Można także ustawić sztywne powiązania pomiędzy adresem IP i adresem sprzętowym. Każda grupa („network", „subnet") ma swoje parametry. Utworzenie nowej grupy (np. „subnet" w obrębie „network") powoduje skopiowanie wszystkich parametrów z grupy nadrzędnej (np. jeśli sieć „lan" ma parametr „domain-name", to po dodaniu podsieci „local" jest on do niej automatycznie kopiowany - później może być zmieniony lub usunięty)
- na początku dla każdego interfejsu należy utworzyć „network" (w przykładzie powyżej są to „wan" i „lan")
- w każdym „network" należy dodać podsieci IP takie, jakie występują w tej sieci (nie muszą one być dostępne z routera ważne, żeby były w tej samej fizycznej sieci)
- w tym momencie można już dodawać zakresy adresów IP i sztywne powiązania adres IP - adres sprzętowy

3.3.5.3

3.3.5.3. dhcp [on | off | relay]

Serwer DHCP/BOOTP może pracować w trzech trybach:

- **on** - serwer jest włączony i odpowiada na zapytania z podsieci
- **off -** serwer jest wyłączony

- **relay -** serwer jest wyłączony, a aktywny jest Relay Agent przekazujący zapytania z podsieci do innego serwera DHCP

3.3.5.4. dhcp add

Polecenie **dhcp add** pozwala na dodawanie sieci, podsieci, zakresów adresów IP, itp. Może przybrać następujące formy:

- **dhcp add network <nazwa>**

Dodaje nową sieć podłączoną do interfejsu routera. Sieci powinno być tyle, ile interfejsów. Powiązanie sieć - interfejs jest dokonywane później, przy dodawaniu podsieci IP.

```
dhcp add network lan
```

- **dhcp add subnet <nazwa> <sieć> <adres> <maska>**

Dodaje nową podsieć IP do danej sieci. Dla każdej podsieci podłączonej do interfejsu LAN lub WAN należy dodać podsieć IP (z takimi adresami, jakie są na danym interfejsie). Dodatkowo można dodać inne podsieci IP nie skonfigurowane na żadnym interfejsie, a znajdujące się w tej samej sieci lub znajdujące się za DHCP Relay'em.

```
dhcp add subnet local lan 10.0.0.0 255.0.0.0
```

- **dhcp add host <nazwa> <adres mac> <adres ip>**

Polecenie pozwala statycznie powiązać adres sprzętowy (MAC) z adresem IP. Adres IP musi należeć do jednej z wpisanych podsieci. Podanemu adresowi sprzętowemu będzie przydzielany wyłącznie ten adres IP:

```
dhcp add host serwer 00:50:13:2e:15:ca 10.0.0.5
```

- **dhcp add range <adres początkowy> <adres końcowy>**

Polecenie dodaje zakres adresów IP, które będą przydzielane stacjom w sieci. Zakres adresów musi się w całości mieścić w jednej z utworzonych podsieci.

```
dhcp add range 10.0.0.5 10.0.0.37
```

- **dhcp add option <opcja> <wartość>**

Polecenie dodaje opcję globalną przekazywaną klientowi do początkowej konfiguracji. Dostępne opcje to m.in.

- **routers** - bramki w danej podsieci (zazwyczaj należy definiować osobne bramki dla każdej podsieci, a nie globalnie)
- **domain-name -** nazwa domeny
- **domain-name-servers -** adresy serwerów DNS
- **filename -** nazwa pliku zawierającego system operacynjy
- **next-server -** serwer, z którego plik będzie ściągany przez TFTP

```
dhcp add option domain-name tahoe.pl
```

- **dhcp add relay <adres> [<port>]**

Pozwala dodać adres serwera DHCP, używanego gdy router pracuje jako DHCP Relay Agent. Zapytania przychodzące z podłączonej do routera podsieci są przekazywane do tego serwera. Parametr <port> Jest opcjonalny, domyślnie ma wartość 67.

```
dhcp add relay 192.168.0.3
```

3.3.5.5

3.3.5.5. dhcp del

Polecenie pozwala usunąć sieci, podsieci, zakresy IP, itd.

- **dhcp del network <nazwa>**
- **dhcp del subnet <nazwa>**
- **dhcp del host <nazwa>**

Polecenia usuwają odpowiednio sieć, podsieć lub hosta (statyczne powiązanie IP - MAC) o podanej nazwie.

- **dhcp del relay <adres>**

Usuwa serwer DHCP o podanym adresie wykorzystywany w trybie DHCP Relay.

- **dhcp del range <adres początkowy> <adres końcowy>**

Usuwa zakres adresów IP przydzielanych stacjom.

- **dhcp del option <nazwa> <wartość>**

Usuwa opcję globalną. Należy - oprócz nazwy - podać jej wartość, ponieważ niektóre opcje mogą przyjmować kilka wartości (np. serwery DNS, routery, itp.)

3.3.5.6. dhcp rename

3.3.5.6

Polecenie zmienia nazwę sieci, podsieci lub hosta.

- **dhcp rename network <stara nazwa> <nowa nazwa>**
- **dhcp rename subnet <stara nazwa> <nowa nazwa>**
- **dhcp rename host <stara nazwa> <nowa nazwa>**

3.3.5.7. dhcp network/subnet/host

3.3.5.7

Polecenie pozwala dodać lub usunąć opcje sieci, podsieci i hosta. Ma dwie formy:

- **dhcp network add <nazwa opcji> <wartość>**
- **dhcp network del <nazwa opcji> <wartość>**

(zamiast „network" może być „subnet" lub „host", opcje są opisane w p. 3.3.5.2), np. :

```
dhcp network add domain-name tahoe.pl
```

Opcje będą obowiązywać wyłącznie w obrębie danej sieci, podsieci lub hosta. ponadto można ustawić dwa parametry:

- **dhcp network default-lease-time <wartość>**

Ustawia czas (w sekundach), na jaki jest przydzielany adres IP. Po upływie tego czasu komputer musi zgłosić serwerowi, że nadal go używa. Jeśli się nie zgłosi, adres jest uznawany za nieużywany.

- **dhcp network max-lease-time <wartość>**

Stacja (komputer lub inne urządzenie) może zażądać innego czasu przydzielenia adresu IP. Wynegocjowany czas nie będzie większy od powyższego ustawienia

3.3.5.8. dhcp default-lease-time <wartość> dhcp max-lease-time <wartość>

3.3.5.8

Polecenia te działają podobnie, jak opisane w poprzednim punkcie, ale ich znaczenie jest globalne.

3.3.6

3.3.6. exit, quit

Polecenie powoduje rozłączenie z routerem.

3.3.7

3.3.7. fr

Grupa poleceń konfigurujących protokół Frame Relay. Są możliwe następujące parametry:

- **fr ansi**
- **fr q933a**
- **fr cisco -** wybór procedur w kanale kontrolnym Frame Relay (odpowiednio: ANSI T1.617 Annex D, ITU Q.933 Annex A, Cisco® LMI).

- **fr t391 <wartość>** - ustawia parametr T391, tzn. ilość prób nawiązania połączenia w kanale kontrolnym, po których łącze jest uznawane za nieaktywne
- **fr n391 <wartość>** - ustawia parametr N391, tzn. odstęp w sekundach pomiędzy kolejnymi próbami nawiązania połączenia w kanale kontrolnym

- **fr debug on**
- **fr debug off** - włącza i wyłącza wysyłanie przez syslog szczegółów dotyczących pracy łącza Frame Relay

3.3.8

3.3.8. http

Polecenie służy do konfiguracji wbudowanego serwera WWW. Serwer WWW dostępny na porcie 80 pozwala w prosty sposób odczytać statystyki dotyczące pracy routera. Można go włączyć lub wyłączyć wpisując odpowiednio

http on lub **http off**

Dodatkowo można ograniczyć dostęp do niego wpisując:

http host <adres IP>

Wówczas serwer będzie dostępny wyłącznie z wybranego adresu IP. Jeśli jako adres IP zostanie podane 0.0.0.0 to serwer będzie dostępny zewsząd.

3.3.9. ifconfig

Polecenie pozwala skonfigurować interfejsy sieciowe. Są dostępne następujące interfejsy:

- **eth0** - interfejs ethernet
- **eth0:0, eth0:1,** itd**.** - aliasy do interfejsu eth0 (jeden interfejs fizyczny może obsłużyć kilka podsiec iIP)
- **eth0.1, eth0.2,** itd. - sieci VLAN (sieci LAN odseparowane od siebie, choć oparte na tym samym okablowaniu)
- **eth0.1:0, eth0.1:1**, itd. - aliasy do interfejsów VLAN

- **fr1, fr2,** itd. - interfejsy Frame Relay (numer po "fr" jest numerem DLCI)

- **ppp0** - interfejs PPP, używany gdy łącze pracuje w trybie synchronicznego PPP

- **hdlc0** - interfejs HDLC, używany gdy łącze pracuje w trybie Cisco® HDLC

Polecenie ma składnię podobną do komendy „ifconfig" w systemie Linux:

ifconfig <nazwa interfejsu> [<adres ip>] [netmask <maska podsieci>] [bcast <adres broadcast>] [static | dynamic] [bridge { on | off }]

Podanie samego **„ifconfig"** wyświetla informacje o aktywnych interfejsach. Podanie **„ifconfig <nazwa interfejsu>"** wyświetla informacje o danym interfejsie. Wyświetlane są informacje o ustawionym adresie IP, odebranych i wysłanych pakietach, błędach, które pojawiły się podczas transmisji, ilości odebranych i wysłanych bajtów, itp.

Wybranemu interfejsowi można przydzielić adres IP, maskę podsieci i adres broadcast. Można również ustalić, czy włączyć, czy też wyłączyć dynamiczne powiązanie adresów IP z adresami sprzętowymi (dynamiczny lub statyczny ARP).

Przy pomocy parametru **bridge** można ustalić, czy interfejs będzie brany pod uwagę podczas pracy w trybie bridge.

3.3.10. ipchains

Polecenie służy do obsługi firewalla oraz maskarady (NATu) - tj. udostępniania łącza do internetu dla całej podsieci przy wykorzystaniu tylko jednego routowalnego adresu IP.

- **ipchains add** - dodaje wpis na końcu tablicy
- **ipchains insert** - dodaje wpis na początku tablicy
- **ipchains del** - usuwa wpis
- **ipchains list** - wyświetla aktualne ustawienia
- **ipchains flush** - usuwa wszystkie wpisy w tablicy

Po komendzie add, insert lub del należy podać opcje:

- **-s** <podsieć źródłowa>/<maska> [zakres portów]

Określa zakres adresów źródłowych, których dotyczy wpis, jeśli opcja jest pominięta, to wpis dotyczy wszystkich adresów źródłowych.

- **-d** <podsieć docelowa>/<maska> [zakres portów]

Określa zakres adresów źródłowych, których dotyczy wpis, jeśli opcja jest pominięta, to wpis dotyczy wszystkich adresów źródłowych.

- **-p** <protokół> (opcjonalnie)

Opcjonalnie można zawęzić wybór do określonych protokołów.

- **-y** jeśli wpis ma dotyczyć tylko pakietów TCP SYN

Opcjonalnie można zastosować regułę wyłącznie do pakietów TCP SYN (umożliwia to np. zablokowanie wszelkich żądań połączeń przychodzących z zewnątrz przy jednoczesnym dopuszczeniu pakietów zwrotnych do połączeń wychodzących z wewnątrz sieci).

- **-m** <adres IP>

Standardowo maskaradowanemu pakietowi jest przydzielany adres IP z interfejsu, przez który pakiet zostanie następnie wysłany. Przy pomocy powyższej opcji można wymusić użycie innego adresu.

- **accept / deny / masq** - informacja, co zrobić z pakietem, który pasuje do podanych warunków (zaakceptować, odrzucić, maskaradować).

Uwaga! Router wybiera pierwszą regułę z listy, do której pasuje dany pakiet. Tak więc jeśli przed szczegółową regułą znajduje się reguła bardziej ogólna, to ta pierwsza zostanie zastosowana, a ta druga - zignorowana. Widać to dobrze na pierwszym z poniższych przykładów.

Przykładowe komendy:

```
ipchains add -s 215.16.11.0/24 deny
ipchains insert -s 215.16.11.5 accept
```

Wyłącza dostęp dla całej podsieci 215.16.11.0/24 **z wyjątkiem** adresu 215.16.11.5.

Uwaga! Szczegółowa (dotycząca jednego adresu IP) reguła **accept** musi być dodana **przed** ogólną (dotyczącą całej podsieci) regułą **deny** (przy pomocy polecenia insert lub przy pomocy polecenia add wykonanego przed 'add ... deny'). Router wybiera pierwszą regułę z listy, która pasuje do danego pakietu. W przeciwnym wypadku zawsze zastosuje regułę 215.16.11/0 deny i nigdy nie dojdzie do drugiej (akceptującej adres 215.16.11.5).

```
ipchains add d 0.0.0.0/0 80-80 p tcp deny
```

Blokuje dostęp do portu 80 we wszystkich zewnętrznych serwerach

```
ipchains add s 192.168.0.0/16 masq
```

Włącza maskaradę dla podsieci 192.168.0.0/16 (pozostałe adresy nie są maskaradowane)

3.3.11. lang

3.3.11

Pozwala na wybór jezyka, w którym podawane są komunikaty:

- **lang 0 -** polski,
- **lang 1** - angielski.

3.3.12. masq

3.3.12

Polecenie „masq" wyświetla listę maskaradowanych połączeń. Lista zawiera adresy źródłowe i docelowe połączeń, port przyporządkowany im przez router, czas, jaki pozostał do wykasowania

wpisu z tablicy oraz ilość wolnych pozycji w tablicy, które można przeznaczyć na nowe połączenia. Adresy IP i porty są podane w postaci liczb szesnastkowych.

3.3.13

3.3.13. mem

„Mem" wyświetla statystyki wykorzystania pamięci RAM. Istotna jest pozycja „free malloc" określająca ilość wolnej pamięci.

3.3.14

3.3.14. ping

„Ping" pozwala sprawdzić dostępność urządzenia o podanym adresie IP, na przykład:

```
ping 10.0.0.2
```

podaje czas przesyłania pakietu do stacji 10.0.0.2 i z powrotem lub informuje o jego niedostępności.

3.3.15

3.3.15. ppp

Polecenie pozwala skonfigurować łącze pracujące w trybie synchronicznego PPP. Dostępne są następujące opcje:

- **ppp defroute on**
- **ppp defroute off** - polecenie odpowiednio włącza i wyłącza dodawanie domyślnego routingu przez interfejs PPP po nawiązaniu połączenia
- **ppp mtu <wartość>** - ustawia maksymalny rozmiar pakietu, jaki router zgodzi się wysyłać przez łącze ppp (ostateczne MTU zależy od ustawienia MRU na zdalnym routerze)
- **ppp mru <wartość>** - ustawia maksymalny rozmiar pakietu, jaki router może odebrać przez łącze PPP (ma wpływ na negocjację MTU na łączu)
- **ppp ip <adres lokalny>:[<adres zdalny>]** - ustawia adresy IP (lokalny, opcjonalnie zdalny) używane w czasie negocjacji połączenia PPP
- **ppp up1 <komenda>**
- **ppp up2 ... -** opcje od „up1" do „up4" pozwalają wpisać maksymalnie 4 polecenia uruchamiane w momencie nawiązania połączenia PPP
- **ppp down1 <komenda>**
- **ppp down2 ...**- opcje od „down1" do „down4" pozwalają wpisać maksymalnie 4 polecenia uruchamiane w momencie przerwania połączenia PPP

- **ppp user**- ustawia nazwę użytkownika wykorzystywaną w czasie autoryzacji (jeśli zdalny router tego wymaga)
- **ppp password**- ustawia hasło wykorzystywane w czasie autoryzacji (jeśli zdalny router tego wymaga)
- **ppp debug on**
- **ppp debug off**- odpowiednio włącza i wyłącza wysyłanie przez syslog szczegółowych informacji o negocjacji połączenia i pracy łącza PPP

3.3.16. ps

3.3.16

Wyświetla listę i stan działających procesów.

3.3.17. reboot

3.3.17

Polecenie powoduje restart całego routera.

3.3.18. route

3.3.18

Polecenie **route** jest podobne do analogicznej komendy w systemie Linux i służy do konfiguracji routingu. Wpisanie samego „route" pokazuje aktualną tablicę routingu. Są dostępne następujące parametry:

- **route add <adres> <interfejs>** - dodaje routing do wybranego adresu bezpośrednio przez podany interfejs (stacja o tym adresie musi być w podsieci bezpośrednio podłączonej do interfejsu)
- **route add <adres> gw <bramka>** - dodaje routing do wybranego adresu przez podaną bramkę
- **route add -net <adres> netmask <maska> <interfejs>** - dodaje routing do podsieci o podanym adresie i masce bezpośrednio przez dany interfejs
- **route add -net <adres> netmask <maska> gw <bramka>** - dodaje routing do podsieci o podanym adresie i masce przez wybraną bramkę
- **route add default gw <adres>** - dodaje routing domyślny przez wybraną bramkę
- **route del <adres>** - usuwa routing do danego adresu IP
- **route del -net <adres> netmask <maska> -** usuwa routing do podanej podsieci
- **route del default -** usuwa routing domyślny

3.3.19. serial

Polecenie pozwala skonfigurować tryb pracy portu szeregowego V.35:

- **serial fr** - Frame Relay
- **serial ppp -** synchroniczne PPP
- **serial hdlc -** Cisco® HDLC

3.3.20. snmp

Polecenie umożliwia konfigurację obsługi protokołu SNMP (Simple Network Management Protocol). Są możliwe następujące użycia:

- **snmp** wyświetla aktualną konfigurację:

```
Tahoe> snmp
SNMP on
Read community: public
Write community: private
SNMP host1: <any>
SNMP host2: <disabled>
SNMP host3: <disabled>
```

- **snmp on -** włącza obsługę SNMP
- **snmp off** - wyłącza obsługę SNMP
- **snmp rdcomm <tekst**> - ustawia read community - hasło potrzebne do odczytu parametrów przez SNMP
- **snmp wrcomm <tekst>** - ustawia write community - hasło pozwalające na zmianę paramterów przez SNMP
- **snmp host1 <adres>**
- **snmp host2 <adres>**
- **snmp host3 <adres>** - umożliwia ustawienie 3 adresów, z których będzie możliwe konfigurowanie przez SNMP. Wpisanie 0.0.0.0 umożliwia dostęp z dowolnego adresu. Wpisanie 255.255.255.255 wyłącza dany wpis (wpisanie 255.255.255.255 we wszystkie trzy miejsca jest równoznaczne z wyłączeniem obsługi SNMP)

3.3.21. strictarp

Polecenie „strictarp" pomaga zabezpieczyć się przed osobami nielegalnie podłączającymi się do sieci LAN (np. do sieci osiedlowych). Po włączeniu tego trybu (przy użyciu „**strictarp on**") i wpisaniu do tablicy

ARP statycznych powiązań IP-MAC router zaczyna nasłuchiwać zapytań ARP o adresy, które ma wpisane statycznie. Jeśli zapytanie przyjdzie spod adresu MAC innego niż w tablicy ARP routera, router wysyła odpowiedź z właściwym adresem MAC.

Takie zapytanie jest wysyłane przez komputer pracujący pod Microsoft® Windows™ podczas startu systemu. Po uzyskaniu odpowiedzi od routera użytkownikowi pojawi się komunikat, informujący że wybrany adres IP jest zajęty, co uniemożliwi korzystanie z sieci pod „nielegalnym" adresem. Tryb „strictarp" można wyłączyć wpisując „**strictarp off**".

3.3.22. syslog

3.3.22

Router może wysyłać komunikaty o swojej pracy do serwera syslog. Polecenie ma następującą składnię:

- **syslog on** - włącza logowanie
- **syslog off** - wyłącza logowanie
- **syslog host <adres ip>** - ustawia adres IP serwera, do którego są wysyłane komunikaty

3.3.23. telnet

3.3.23

Polecenie pozwala kontrolować dostęp do routera przez telnet. Dostęp ten można włączyć lub wyłączyć wpisując odpowiednio

telnet on lub **telnet off**

Dodatkowo można ograniczyć dostęp do niego wpisując:

telnet host <adres IP>

Wówczas serwer telnet jest dostępny wyłącznie z wybranego adresu IP. Jeśli jako adres IP zostanie podane **0.0.0.0** to router będzie dostępny zewsząd.

3.3.24. tftp

3.3.24

Polecenie umożliwia konfigurację serwera TFTP służącego do aktualizacji oprogramowania systemowego (firmware). Są możliwe trzy użycia:

- **tftp on** - włącza serwer TFTP
- **tftp off** - wyłącza serwer TFTP

- **tftp host <adres ip>** - jeśli serwer jest włączony, to dostęp do niego jest możliwy tylko z podanego adresu IP. Jeśli podany zostanie adres 0.0.0.0, dostęp będzie możliwy z dowolnego adresu.

3.3.25

3.3.25. timeout

Polecenie pozwala ustalić, po jakim czasie nieaktywności użytkownika sesja telnet jest rozłączana. Ma następującą składnię:

timeout <w czasie sesji> [<w czasie logowania>]

Pierwszy parametr jest czasem niektywności użytkownika (w sekundach) po jakim połączenie jest rozłączane. Drugi, opcjonalny parametr, dotyczy nieaktywności w czasie logowania. Wpisanie „0" jako jednego z tych czasów powoduje usunięcie danego ograniczenia.

Ustawienia dotyczą również dostępu przez konsolę, jeśli jest on chroniony hasłem (polecenie „console passwd on").

3.3.26

3.3.26. uptime, w

Wyświetla informację ile czasu minęło od ostatniego restartu routera.

3.3.27

3.3.27. user

Polecenie **user** służy do zarządania użytkownikami mającymi dostęp do routera. Router może pracować w dwóch trybach:

- jeden użytkownik - do dostępu do routera jest potrzebne tylko hasło. Użytkownik logując się otrzymuje pełny dostęp do urządzenia
- wielu użytkowników - można utworzyć kilku użytkowników o różnych nazwach i z różnymi hasłami. Dodatkowo mogą oni mieć różne uprawnienia, np. tylko do odczytu konfiguracji, bez prawa modyfikacji

Polecenie **user** może posiadać następujące parametry:

- **user list** - wyświetla listę użytkowników
- **user add <nazwa> -** dodaje nowego użytkownika
- **user del <nazwa> -** usuwa użytkownika
- **user passwd <nazwa> <hasło>** - zmienia hasło użytkownika
- **user level <nazwa> <poziom dostępu>** - zmienia użytkownikowi poziom dostępu do routera. Parametr <poziom

dostępu> może przyjąć wartość:

- **admin** - pełny dostęp do routera
- **read-only** - pozwala jedynie na odczyt konfiguracji i statystyk

- **user mode { single | multi }** - służy do przełączania pomiędzy trybem jednego użytkownika (**single**) a trybem wielu użytkowników (**multi**)

3.3.28. ver

3.3.28

Wyświetla aktualną wersję oprogramowania.

3.3.29. watchdog

3.3.29

Komenda "watchdog" pozwala dodatkowo zabezpieczyć się przed nieprzewidzianymi problemami w pracy routera. Router przy pomocy polecenia "ping" sprawdza dostępność wybranych adresów IP i resetuje się, jeśli choć jeden z tych adresów nie odpowiada.

Polecenie ma następującą składnię:

- **watchdog on** - włącza watchdoga
- **watchdog off** - wyłącza watchdoga
- **watchdog <przerwa> <ilość> <czas> <IP> [<dodatkowy IP>]** - konfiguruje watchdoga. Po upłynięciu **<przerwa>** sekund router wysyła do adresu **<IP>** (a także do **<dodatkowy IP>**, jeśli taki jest skonfigurowany) **<ilość>** pakietów w odstępach **<czas>** sekund. Jeśli na żaden pakiet nie przyjdzie odpowiedź, router jest automatycznie restartowany.

3.3.30. write

3.3.30

Zapisuje wszystkie ustawienia do pamięci EEPROM oraz wyświetla iinformację, ile zostało w niej wolnego miejsca. W przypadku przepełnienia pamięci EEPROM należy usunąć część konfiguracji, np. statyczne wpisy ARP, opcje lub zakresy DHCP, itd.

4. Konfiguracja do pracy z siecią Polpak-T

Poniżej przedstawiony jest opis dwóch wariantów konfiguracji routera do współpracy z siecią Polpak-T.

4.1. Dostęp do Internetu

Po zestawieniu łącza do sieci Polpak-T użytkownik zazwyczaj otrzymuje kilka informacji na jego temat. Oto przykład:

```
Sygnalizacja:            ANSI
Numer DLCI:              99
Adres routera TP S.A.:   194.204.100.129
Adres routera klienta:   194.204.100.130
Podsieć na łączu:        194.204.100.128
Maska podsieci:          255.255.255.252
```

Na początku należy upewnić się, że port V.35 pracuje w trybie Frame Relay:

```
Tahoe> serial fr
```

Następnie należy skonfigurować interfejs Frame Relay nadając mu adres przydzielony dla klienta. W przypadku DLCI 99 będzie to interfejs **fr99**. Ponadto trzeba dodać routing domyślny przez ten właśnie interfejs:

```
Tahoe> ifconfig fr99 194.204.100.130
Tahoe> route add default fr99
```

W tym momencie ping do routera TP S.A. powinien już działać. Pozostaje skonfigurowanie sieci lokalnej. Jeśli klient wystąpił o przyznanie puli adresów IP, to musi je ustawić na interfejsie eth0. Przykładowo dla podsieci 212.244.1.0 i masce podsieci 255.255.255.0 należy wpisać:

```
Tahoe> ifconfig eth0 212.244.1.1 netmask
255.255.255.0
```

Uwaga! Po zmianie adresu IP na eth0 router przestanie być dostępny pod starym adresem (10.0.0.1). Dlatego w przypadku konfiguracji przez telnet trzeba się z nim połączyć ponownie pod nowym adresem IP. Nie jest to konieczne podczaskonfiguracji przez port konsoli szeregowej.

Komputery w sieci powinny otrzymać kolejne adresy, tj. 212.244.1.2, 212.244.1.3, itd., maskę podsieci 255.255.255.0, a jako domyślną bramkę należy ustawić IP routera, czyli 212.244.1.1.

Jeśli klient nie otrzymał dodatkowej puli adresów IP może wykorzystać w swojej podsieci tzw. adresy prywatne, np. podsieć 10.0.0.0, 192.168.0.0 i inne, a następnie włączyć maskaradę. Na przykład w przypadku użycia podsieci 10.0.0.0 należy wpisać:

```
Tahoe> ipchains add -s 10.0.0.0/8 masq
```

Zmiana konfiguracji interfejsu eth0 nie jest w tym przykładzie wymagana. Komputery w sieci powinny otrzymać adresy 10.0.0.2, 10.0.0.3, itd., maskę podsieci 255.0.0.0, a jako domyślną bramkę należy ustawić IP routera, czyli 10.0.0.1.

Po skonfigurowaniu routera ustawienia należy zapisać do pamięci EEPROM:

```
Tahoe> write
```

4.2. Sieć prywatna

Załóżmy, że są dwa oddziały firmy połączone kanałem PVC przez sieć Polpak-T. Jedna z nich używa adresów z podsieci 192.168.1.0 (maska 255.255.255.0), a druga 192.168.2.0 (identyczna maska). TP S.A. przydzieliła w pierwszej lokalizacji DLCI 101, a w drugiej DLCI 102 (ten sam kanał PVC może mieć różne identyfikatory DLCI w różnych miejscach).

W pierwszej lokalizacji należy skonfigurować interfejs fr101 i dodać routing do zdalnej podsieci. Adres IP użyty na interfejsie fr101 jest nieistotny, ale dobrze użyć tego samego adresu, który jest na interfejsie eth0.

```
Tahoe> ifconfig fr101 192.168.1.1
Tahoe> route add -net 192.168.2.0 netmask
255.255.255.0 fr101
```

Ponadto należy skonfigurować interfejs eth0:

```
Tahoe> ifconfig eth0 192.168.1.1 netmask
255.255.255.0
```

W drugiej lokalizacji konfiguracja jest bardzo podobna:

```
Tahoe> ifconfig fr102 192.168.2.1
Tahoe> route add -net 192.168.1.0 netmask
255.255.255.0 fr102
Tahoe> ifconfig eth0 192.168.2.1 netmask
255.255.255.0
```

Jeśli dodatkowo jest wykorzystywany dostęp do internetu (zazwyczaj przez DLCI 99), to można skonfigurować interfejs fr99 i ustawić przez niego domyślny routing.

Na koniec ustawienia należy zapisać do pamięci EEPROM:

```
Tahoe> write
```

5. Dane techniczne

- procesor:
  Motorola MC68302, 20MHz

- protokoły sieciowe:
  IP, TCP, UDP, ICMP, TFTP, SNMP, DHCP, BOOTP, RFC-1490, PPP, Frame Relay, Cisco® HDLC, IEEE 802.1q

- sygnalizacja FR:
  ANSI T1.617 Annex A, ITU Q.933 Annex D, Cisco® LMI

- interfejs Ethernet:
  Tahoe® 1801: 10BaseT, złącze RJ45
  Tahoe® 1808: 10/100BaseT, 8 złącz RJ45

- konsola szeregowa:
  RS-232, 9600 b/s, 8N1, złącze DB9/M

- wymiary:
  229 mm (szer.) x 57 mm (wys.) x 152 mm (dł.)

- zasilanie i pobór mocy:
  Tahoe® 1801: 7.5V, 400 mA, 3W
  dołączony zasilacz 230V/50Hz
  Tahoe® 1808: 7.5V, 1.2A, 9W
  dołączony zasilacz 230V/50Hz

- warunki klimatyczne:

przechowywanie:	temperatura	-20°C do 65**°C**
	wilgotność	5 do 95%
praca:	temperatura	0°C do 40°C
	wilgotność	0 do 85%

6. Deklaracja zgodności

CE

TAHOE
Piotr Kaczmarzyk
ul. Uniwersytecka 1
50-951 Wrocław, Polska

Deklaruję, że produkty Tahoe 1801 i Tahoe 1808 są zgodne z następującymi dyrektywami Unii Europejskiej:

- **73/23/EEC** dyrektywa niskonapięciowa
- **89/336/EEC** kompatybilność elektromagnetyczna
- **99/5/EEC** wymagania dla radiowych i telekomunikacyjnych urządzeń końcowych

Zgodność Tahoe 1801 i Tahoe 1808 z wymaganiami powyższych dyrektyw została zapewniona przez kompletne zastosowanie następujących norm zharmonizowanych :

- **EN 60950:2000**
- **EN 55022:1998**
- **EN 61000-6-1:2002**
- **EN 61000-6-3:2002**

Podpisano: Piotr Kaczmarzyk
Stanowisko: Dyrektor

Podpis: Piotr Kaczmarzyk

Data: 30 kwietnia 2004
Miejsce: Wrocław, Polska

TAHOE®
ul. Uniwersytecka 1
50-951 Wrocław
tel. (71) 344-26-44
fax (71) 344-26-42
http://www.tahoe.pl/