DEBRANDING ROUTERÓW
ZyXEL P-2602R-D1A / P-2602RL-D1A / Babybox TP

Materiał jest przeznaczony dla byłych klientów Netii i TP S.A., którzy z różnych powodów nie byli w stanie przywrócić w swoim routerze firmowego oprogramowania ZyXel-a (technicy Netii robią to po upływie terminu obowiązywania umowy). Użytkownicy, których nadal obowiązuje umowa, powinni być świadomi tego, że jakakolwiek ingerencja w oprogramowanie routera powoduje utratę praw gwarancyjnych na sprzęt. Ponadto, Babybox (o ile nie zostało to inaczej ustalone w umowie), jest własnością Telekomunikacji Polskiej S.A. i ingerencja w jego firmware może wiązać się z naliczeniem opłaty karnej .
Dodanie nowej sekcji dotyczącej Babybox-a TP i wszystkich późniejszych uwag dotyczących tego modelu (tekst w kolorze zielonym) zawdzięczamy Łukaszowi Rebelińskiemu, który w imponującym tempie dokonał pomyślnego upgrade FW i zechciał podzielić się swoimi doświadczeniami :) .
Pamiętaj, że wszystkie działania podejmujesz na własną odpowiedzialność: błąd przy wykonywaniu procedury możesz przypłacić trwałym unieruchomieniem routera !!! Debranding powoduje również utratę wszelkich ustawień użytkownika, w tym loginów i haseł do VoIP!!!

Potrzebny sprzęt i software to:

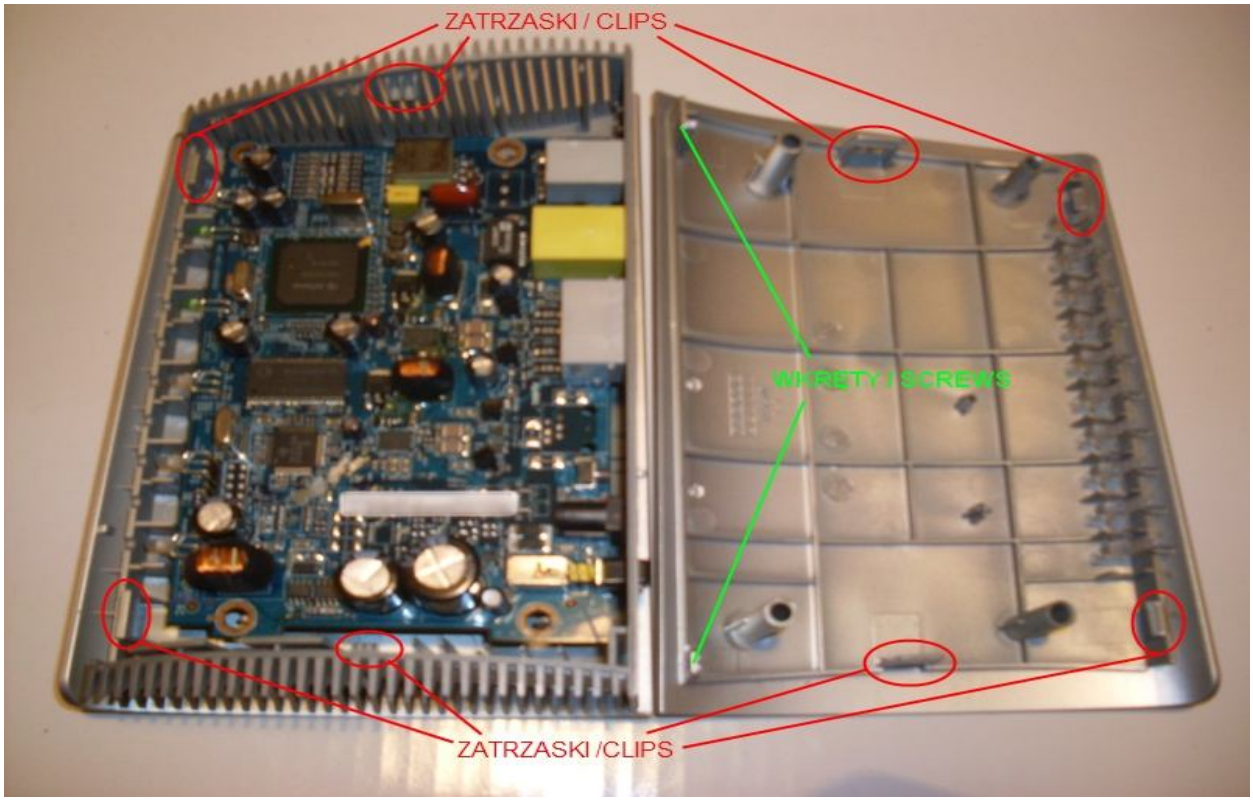
1. Kabelek szeregowy dostosowany do pracy przy poziomach logicznych 0/3,3V (np, od telefonu komórkowego starego typu), opcjonalnie: kabelek USB z emulatorem portu szeregowego.
2. Windowsowy Hyperterminal (jest w systemie);
3. Firmware do routera Zyxel P-2602RL-D1A, dostępne na uploadach firmy;
4. System Windows XP 32-bit i Windows 7 32-bit, na innych systemach nie sprawdzone;
5. Komputer z portem szeregowym (jeśli wykorzystujemy kabelek szeregowy).

Etap backup'u oryginalnego oprogramowania muszę, niestety, pominąć: do jego wykonania potrzebna jest znajomość hasła do telnetu, któe nie jest dostępne w obrandowanych przez Netię routerach. Można je co prawda zdekodować, ale to zupełnie inny temat, który nie będzie tutaj omawiany.

1. Otwieramy router

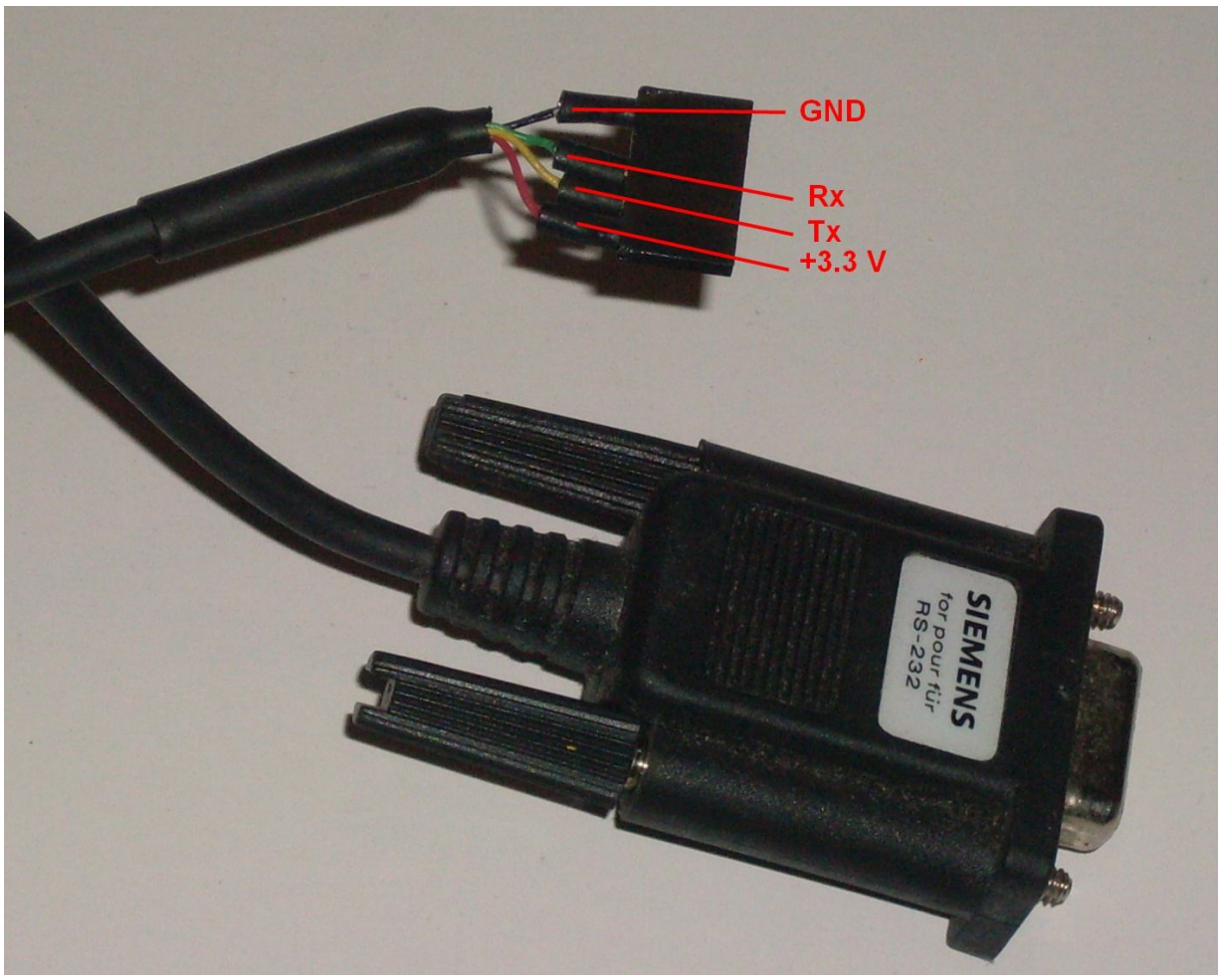
Wizualnie model P2602RL-D1A różni się od P2602R-D1A posiadaniem gniazda telefonii analogowej PSTN, umieszczonego pomiędzy przyciskiem "RESET" a gniazdem "PHONE2". W modelach rozprowadzanych przez Netię gniazdo to – o ile występuje - jest przeważnie zaślepione nalepką "VOID". Babybox TP zgodnie ze stanem mojej wiedzy wydaje się występować tylko w wersji RL.

Po odkręceniu dwóch wkrętów z tyłu urządzenia, zwalniamy ostrożnie cztery zatrzaski uwidocznone na foto.



2. Przygotowujemy kabel szeregowy

Ja osobiście wykorzystałem stary kabel od telefonu Siemens C-25. Po ucięciu wtyczki dolutowałem złącze 1x5 pin (pod tzw. goldpiny). Ze względu na specyficzną budowę tego kabelka (nie jest on zasilany z portu COM tylko z baterii telefonu) musiałem dodatkowo podać mu napięcie zasilające 3,3V z routera.
W przypadku innych kabli może to nie być potrzebne i wykorzystujemy tylko Rx,Tx i GND, wtedy zamiast złącza 1x5 możemy wykorzystać wtyczkę od starego przewodu audio do CD-ROM-u (1x4 pin)



Uwaga! Zamieszczone zdjęcie ma jedynie charakter poglądowy: w zależności od serii produkcyjnej, przewody przyporządkowane do danych sygnałów mogą się różnić kolorami nawet w ramach tego samego modelu kabla, więc koniecznie należy na podstawie tej strony:
http://pinouts.ru/pin_CellularPhonesCables.shtml
zweryfikować "pinologię" złącza i dopiero potem- lutować (THX Łukasz).

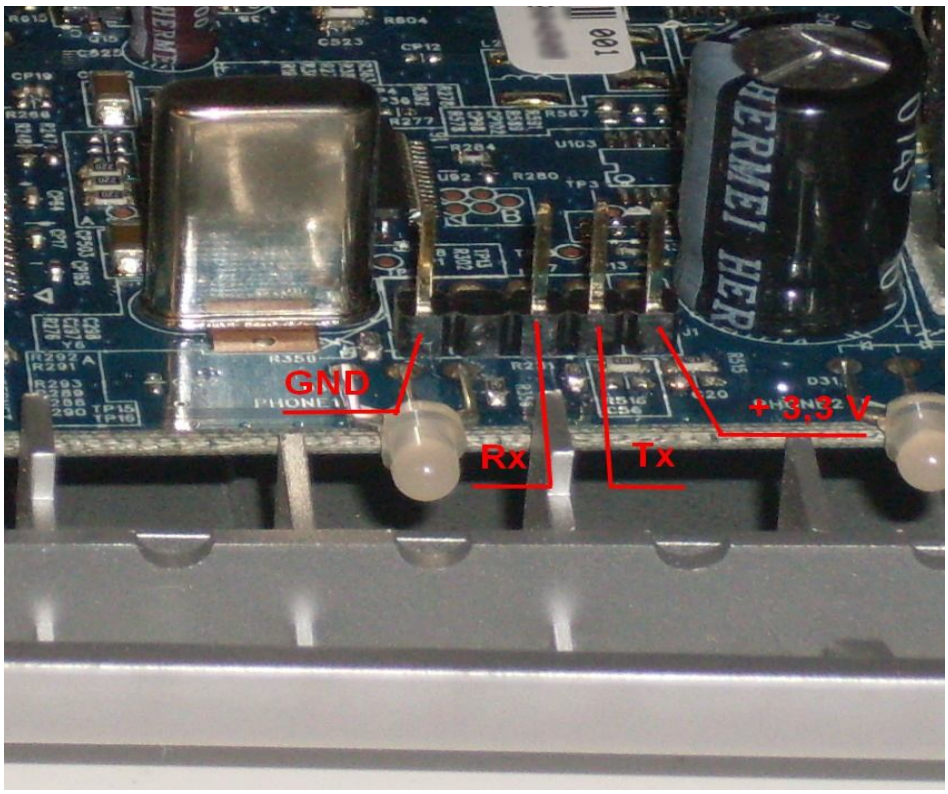
W przypadku zastosowania kabelka Nokii DAU-9P - ze względu na jego minimalistyczną konstrukcję - maksymalna i chyba jedyna działająca prędkość bodowa to 19200 bps. Firmware będzie się wczytywał ok. pół godziny, ale są sygnały, że upgrade przebiega pomyślnie (THX gienek-68).

2a. (Opcjonalnie) Przygotowujemy kabelek USB

Najpopularniejsze typy kabelków USB dostępnych w handlu i sposoby ich przeróbki są opisane pod tym adresem:
http://www.stkaiser.de/anleitung/
w sekcji "USB-Adapter".

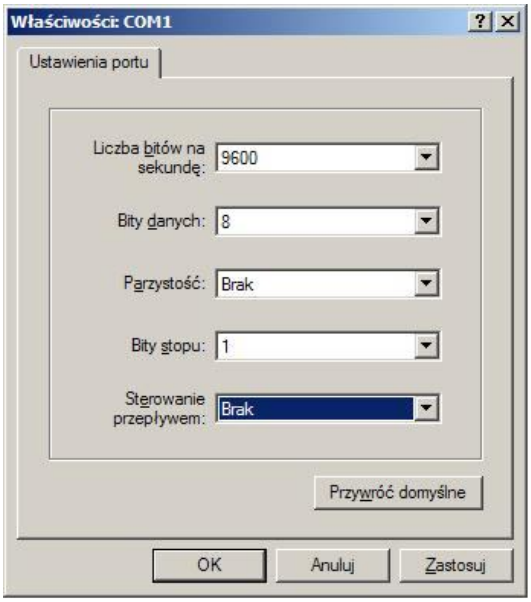
3. **Podłączamy przewód do konsoli routera**

Router jest już przygotowany do tej operacji: ma fabrycznie wlutowane "goldpiny" konsoli. Oczywiście, uważamy, żeby nie pomylić masy z zasilaniem!!! Radzę nawet zaślepić nie używany otworek w złączu od strony kabla- wtedy odwrotne połączenie nie będzie możliwe.

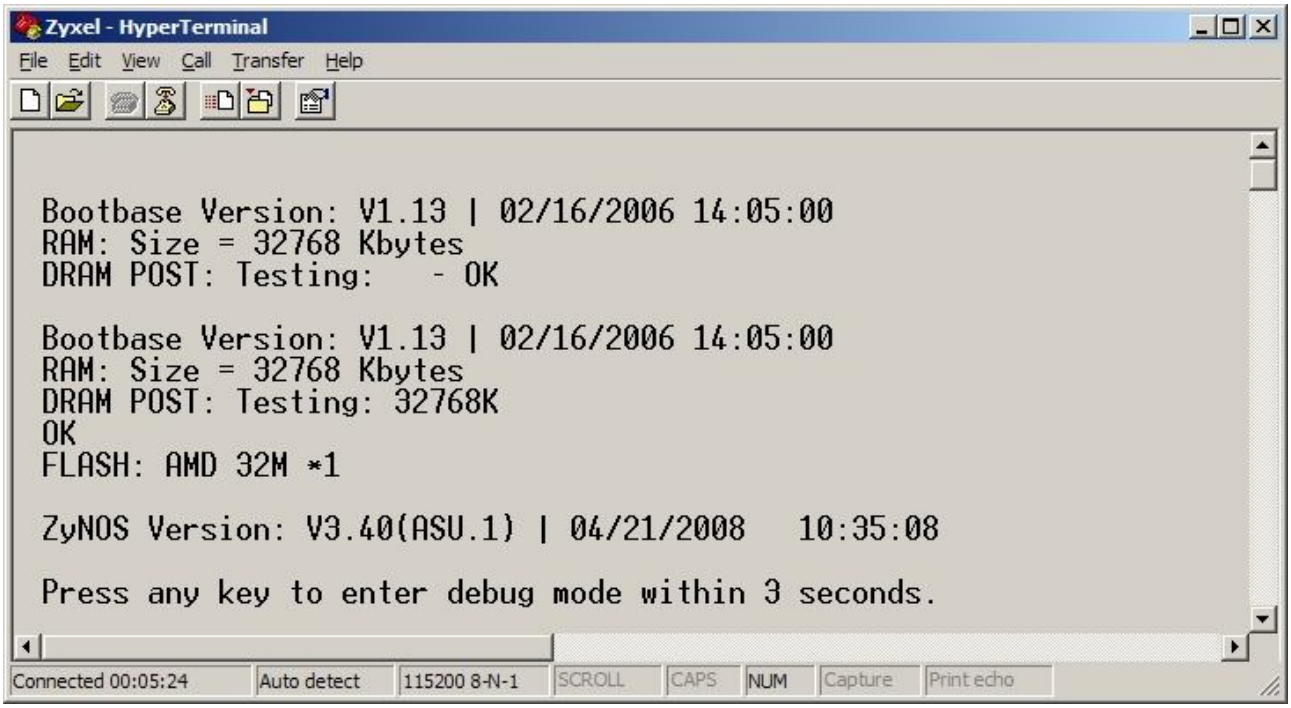


4. **Bootujemy konsolę**

Podłączamy kabel do wyłączonego routera, wywołujemy Hyperterminal (Programy> Akcesoria> Komunikacja).
Tworzymy nowe połączenie o następujących parametrach:

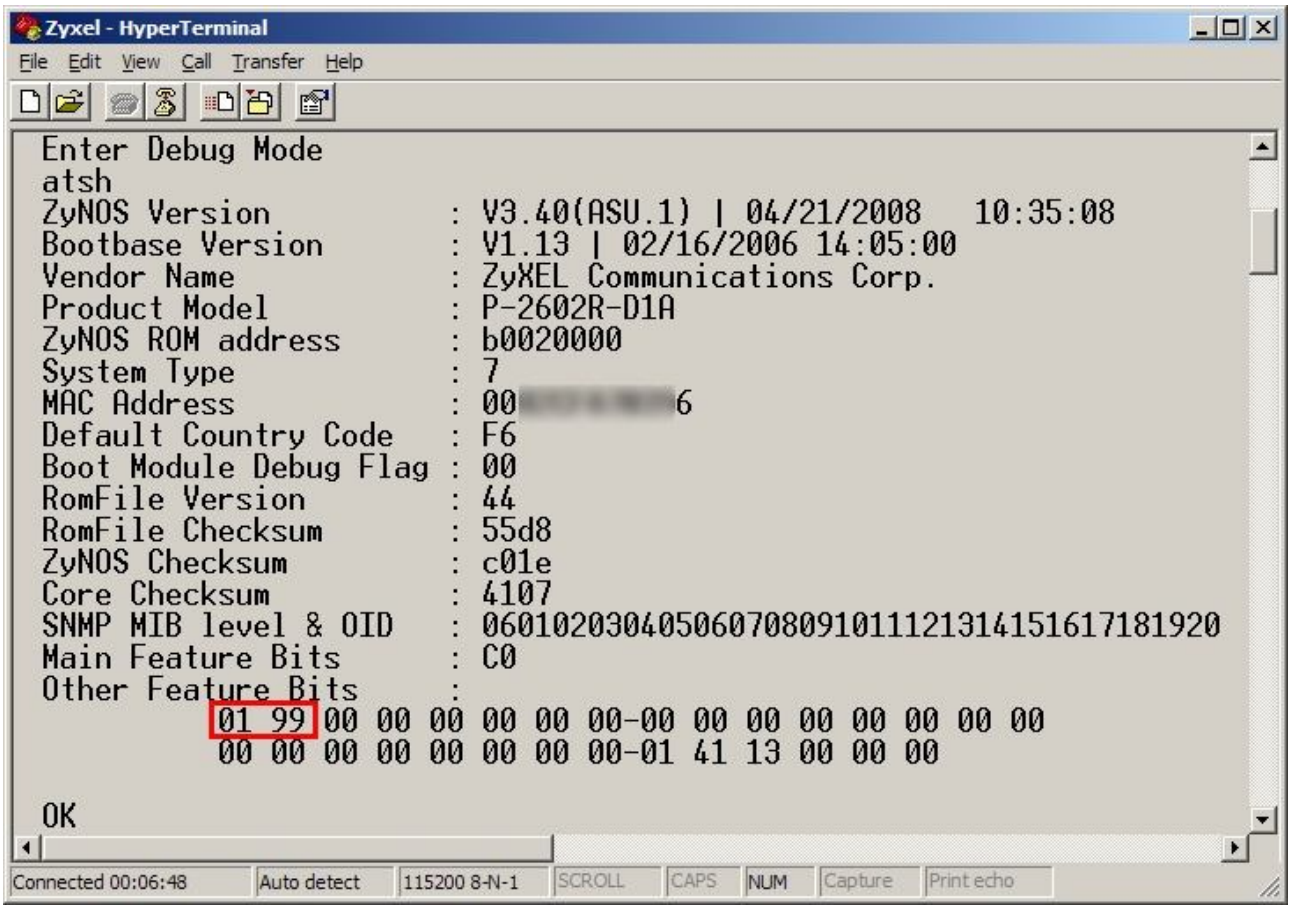


Włączamy router. Powinna prawie natychmiast pojawić się komunikacja. Jeśli tak nie jest, przyczyna tkwi w kablu -być może potrzebne jest zasilanie z routera (wtedy kompletnie brak jekichkolwiek oznak życia) albo błędnie zostały ustawione parametry połączenia.



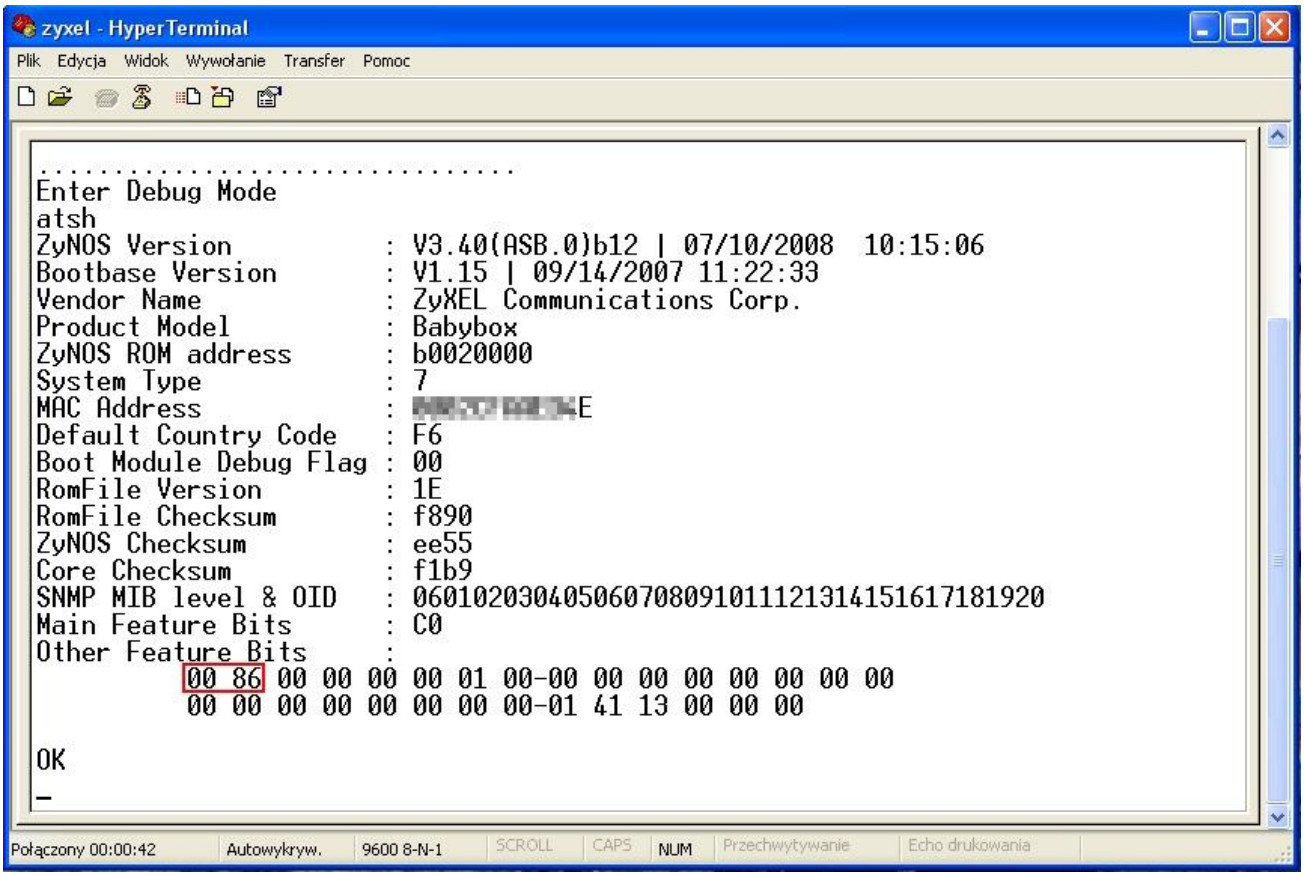
Jeżeli w przeciągu 3 sekund naciśniemy jakiś klawisz, konsola przejdzie do trybu debuggowania. Wpisujemy polecenie (nie jest istotne, czy wprowadzamy małymi, czy dużymi literami- ja wprowadzałem małymi, ale w tekście piszę dużymi, aby małe "L" nie myliło się z jedynką):

ATSH
(dump manufacturer related data in ROM)
i zatwierdzamy "Enterem"



Czerwoną ramką są obwiedzione tzw. feature bits, które są m.in. wyróżnikiem providera, w tym przypadku- Netii.

W przypadku Babybox'a screen wygląda następująco:



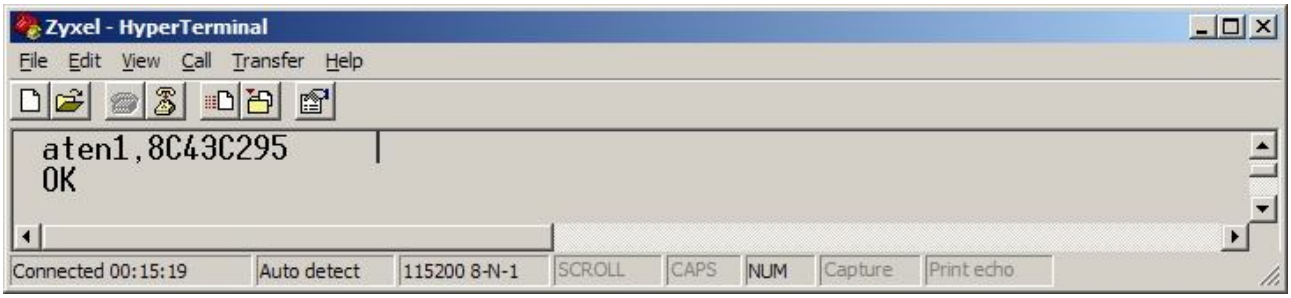
W czerwonej ramce – analogicznie - feature bits ustawione przez TP S.A.

Teraz wprowadzamy konsolę w tryb debuggowania. Aby tego dokonać, musimy wydać odpowiednie polecenie wraz z hasłem. Hasło jest powiązane z ostatnim półbajtem adresu MAC routera. W moim przypadku (patrz screen powyżej) adres kończył się na 6, stąd zgodnie z poniższą tabelą hasło do trybu debug to 8C43C295.

Ostatnia cyfra	Hasło
0 lub 8	10F0A563
1 lub 9	887852B1
2 lub A	C43C2958
3 lub B	621E14AC
4 lub C	310F0A56
5 lub D	1887852B
6 lub E	8C43C295
7 lub F	C621E14A

Wpisujemy polecenie:

ATEN1,<HASŁO>
(set BootExtension Debug Flag)

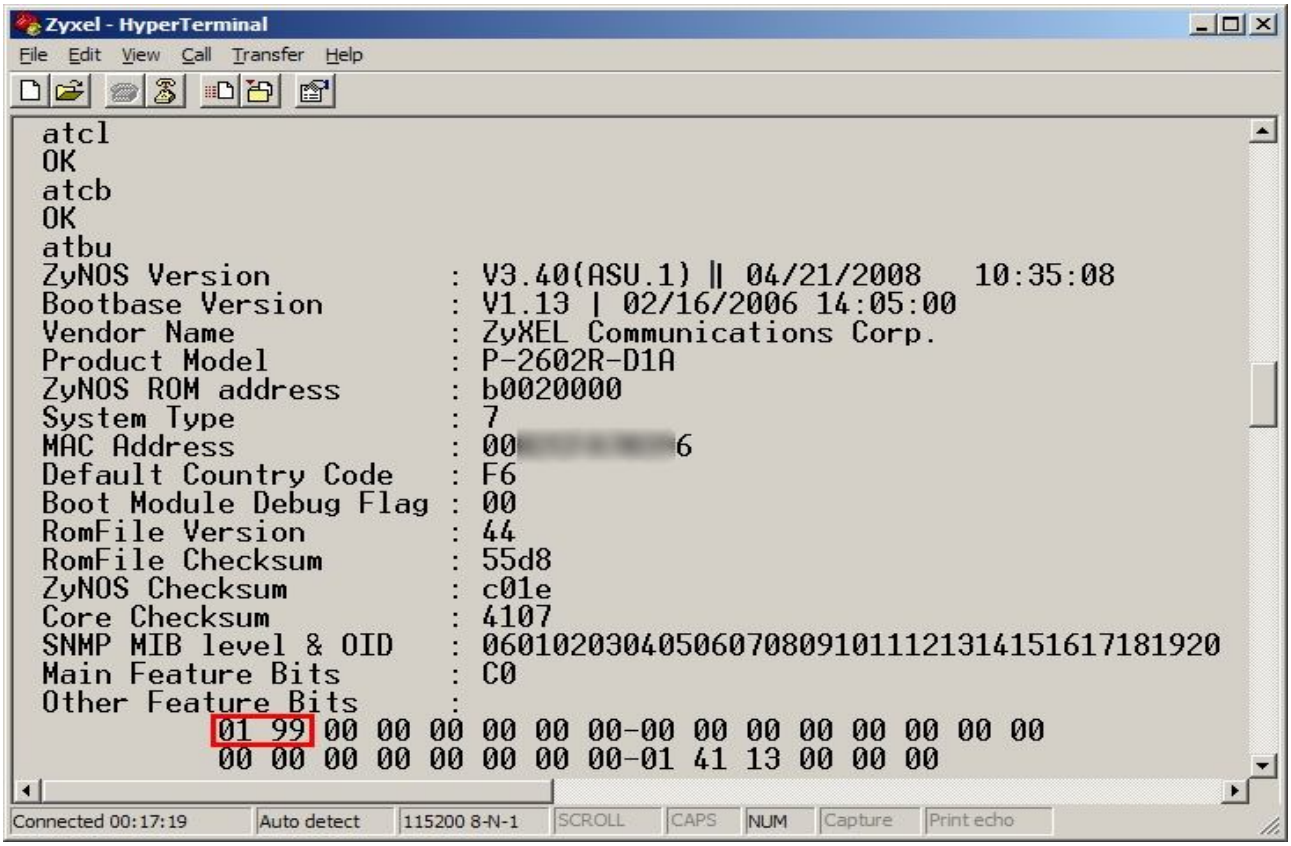


Konsola przeszła do trybu debug.
Teraz tworzymy bufor roboczy, wydając kolejno polecenia:

ATCL
(clear working buffer)

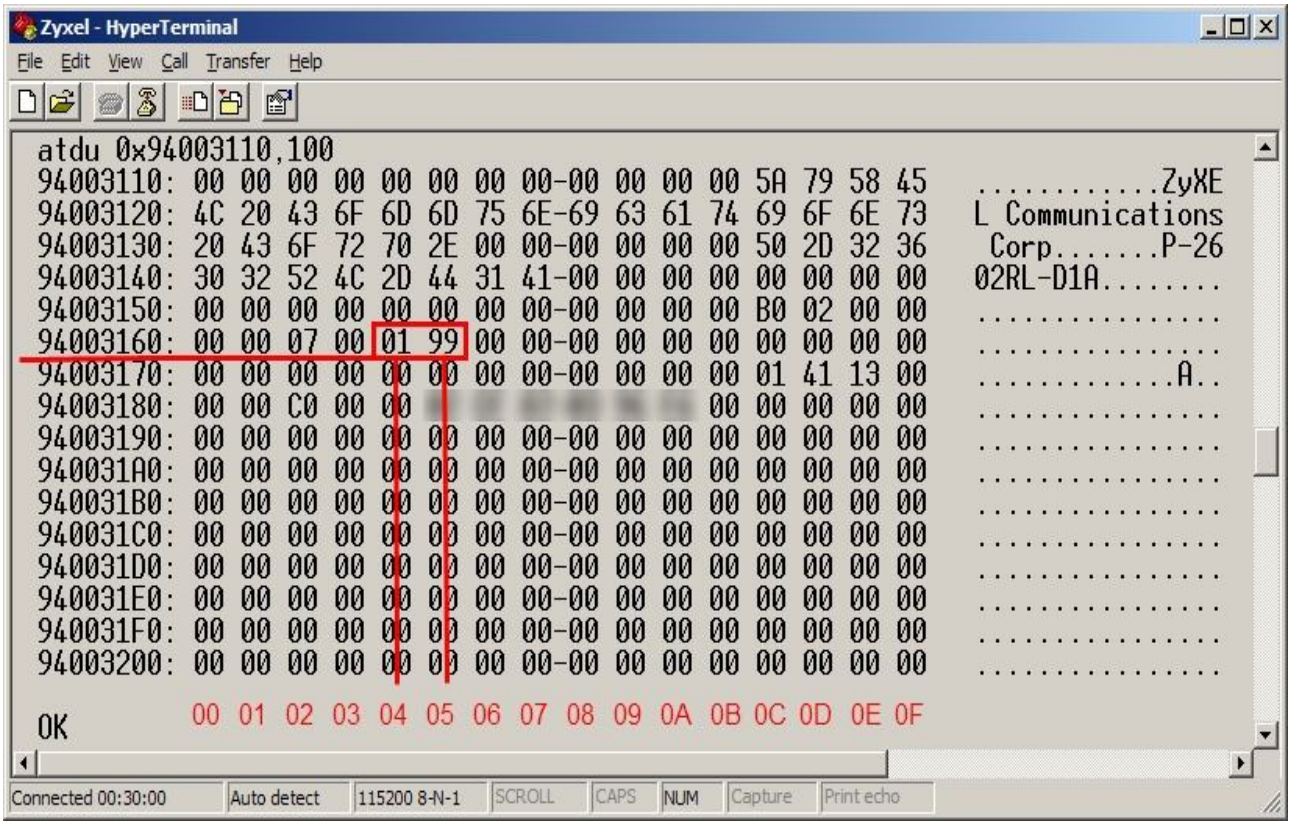
ATCB
(copy from FLASH ROM to working buffer)

ATBU
(dump manufacturer related data in working buffer)



Teraz określamy lokalizację "feature bits" w pamięci RAM, podglądając 100 pierwszych bajtów poczynając od adresu 0x94003110

ATDU 0X94003110,100
(dump memory contents from address 0x94003110 for length 100)



Jak widać powyżej, pierwszy interesujący nas bajt ma adres 0x94003164, a drugi- 0x94003165.
W Babybox-ie poszukujemy oczywiście sekwencji "00 86"

UWAGA: W TWOIM ROUTERZE – W ZALEŻNOŚCI OD WERSJI OPROGRAMOWANIA- TEN ADRES MOŻE BYĆ INNY!!!
POWYŻSZY SCHEMAT PRZEDSTAWIA TYLKO, JAK GO OKREŚLIĆ!!!

Teraz upewniamy się, że dobrze określiliśmy adres, podglądając tylko dwie interesujące nas komórki pamięci z RAM. Odpowiedzią powinny być feature bits- jeśli tak nie jest, liczymy od nowa aż do skutku, bo po modyfikacji niewłaściwej lokacji pamięci ROUTER MOŻE SIĘ NIEODWRACALNIE ZABLOKOWAĆ !!!

ATDU 0X94003164,2

Po uzyskaniu pozytywnej odpowiedzi (01 99, a dla Babybox 00 86) możemy już zmienić zawartość komórek w buforze, aby ustawić feature bits takie, jakie są w "uwolnionym" oprogramowaniu ZyXEL-a, czyli 9D i 17:

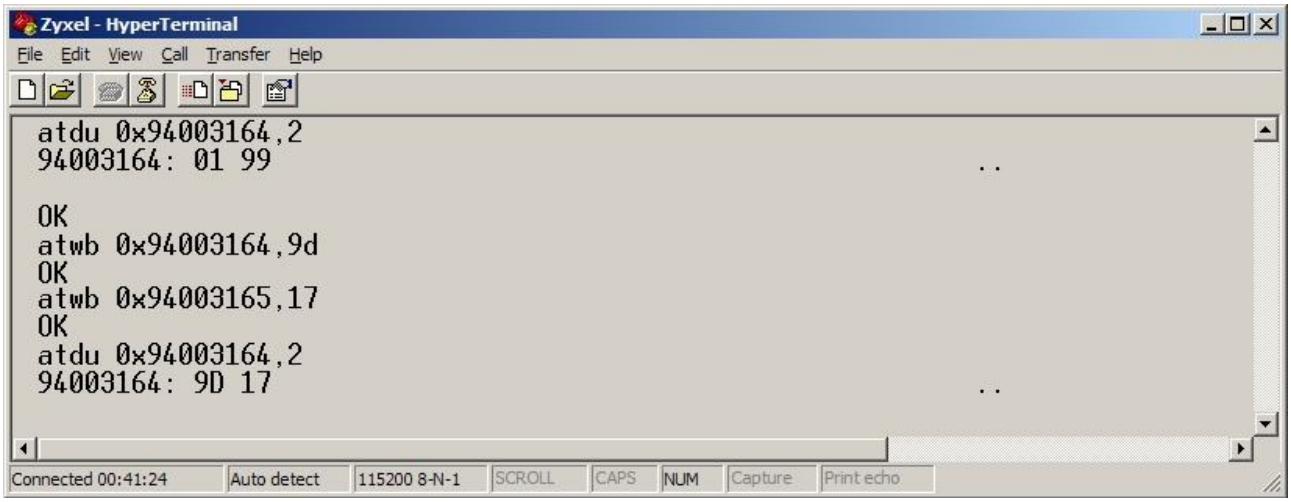
ATWB 0X94003164,9D
(write address 0x94003164 with 16-bit value 9d)

ATWB 0X94003165,17

Teraz upewniamy się, że zawartość interesującej nas lokacji pamięci w buforze została zmieniona:

ATDU 0X94003164,2

Odpowiedzią powinny być zmienione wartości feature bits, czyli 9d i 17



Do tego momentu możemy bezkarnie wyłączać router i powtarzać całą procedurę od nowa bez żadnych konsekwencji. Dalsze działania są nieodwracalne.

Jeśli wszystko jest w porządku, przepisujemy zawartość bufora do pamięci flash:

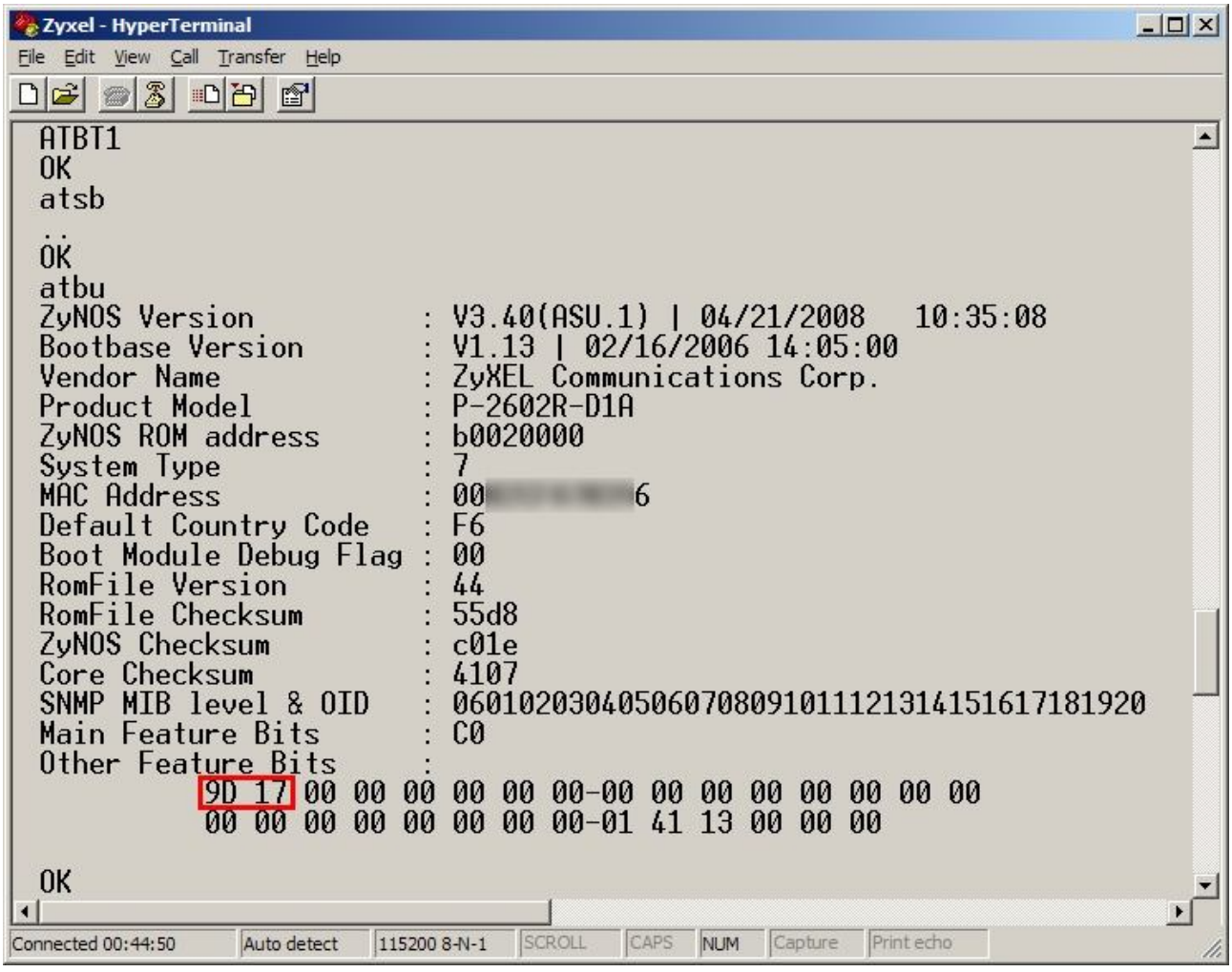
ATBT1

(block0 write enable (1=enable, other=disable))

ATSB
(save working buffer to FLASH ROM)

Flash został zapisany- teraz pozostaje tylko sprawdzić, czy wszystko poszło dobrze, poleceniem:

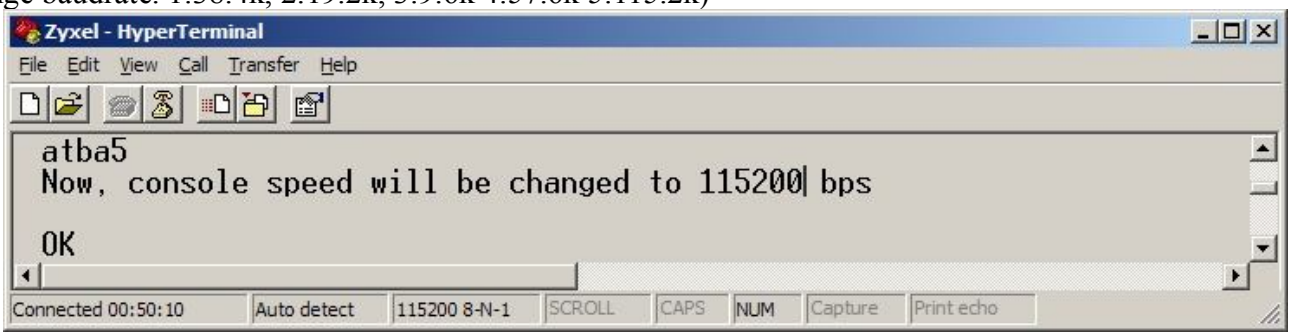
ATBU



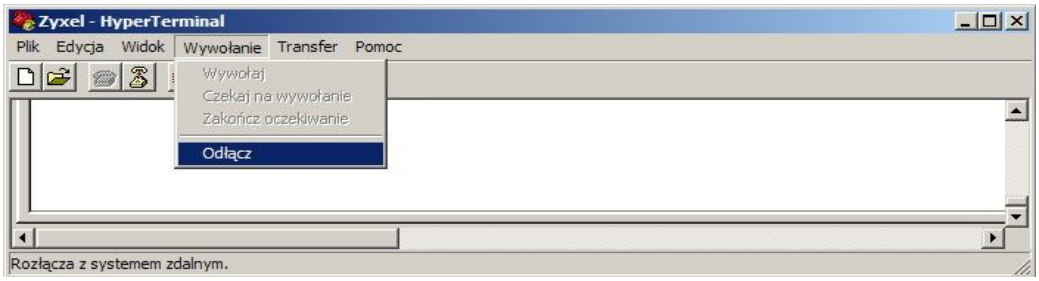
Jak widać, programowanie przebiegło pomyślnie.

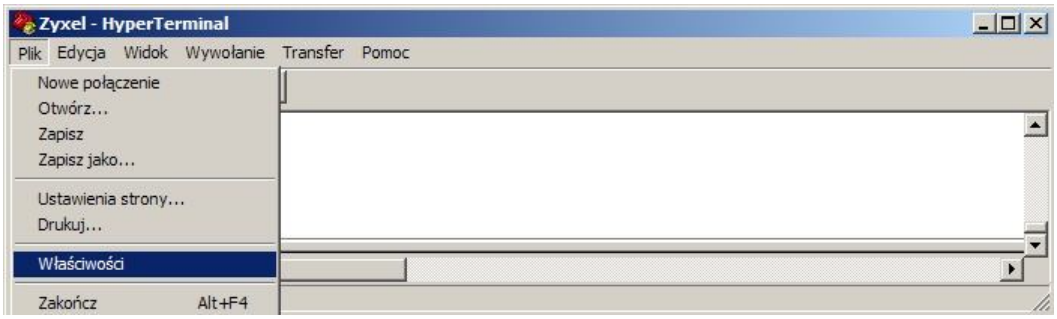
Teraz zwiększamy prędkość konsoli do 115200 bps, aby wgrywanie FW nie trwało wieki :

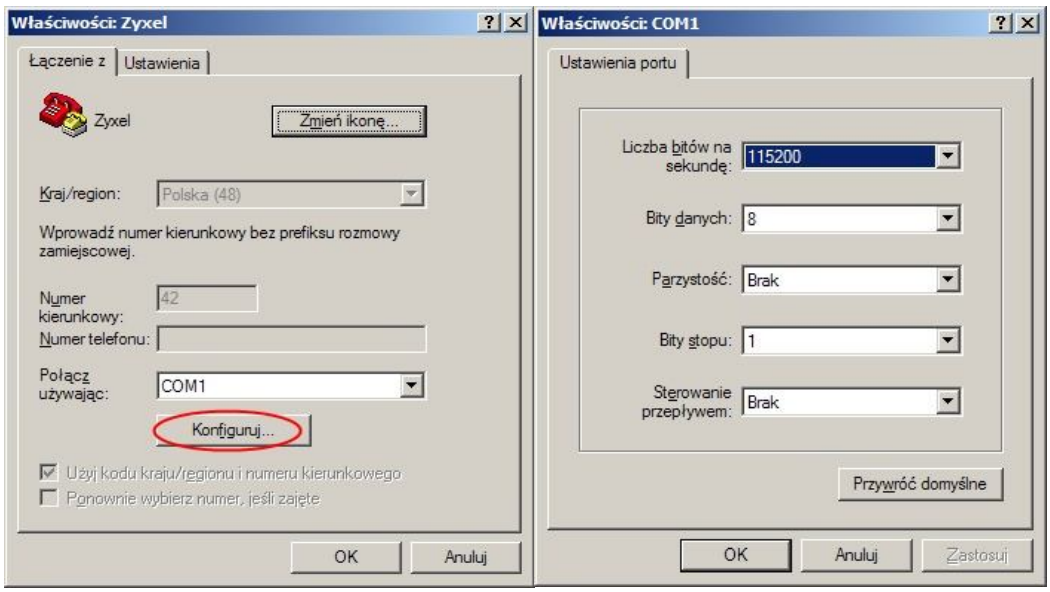
ATBA5 **(Uwaga: dla kabelka DAU-9P wydajemy polecenie ATBA2)**
(change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k)

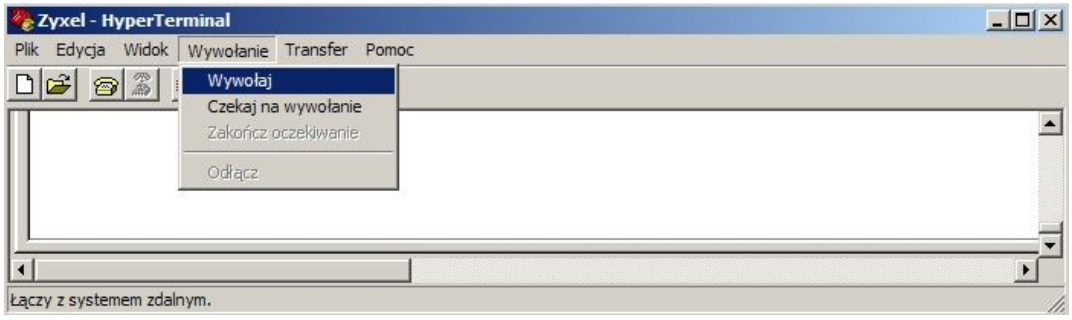


NIE WYŁĄCZAJĄC ROUTERA rozłączamy połączenie w Hyperterminalu (Wywołanie > Odłącz) i zmieniamy prędkość bodową konsoli, również na 115200 (Plik > Właściwości >Konfiguruj). Łączymy się ponownie.





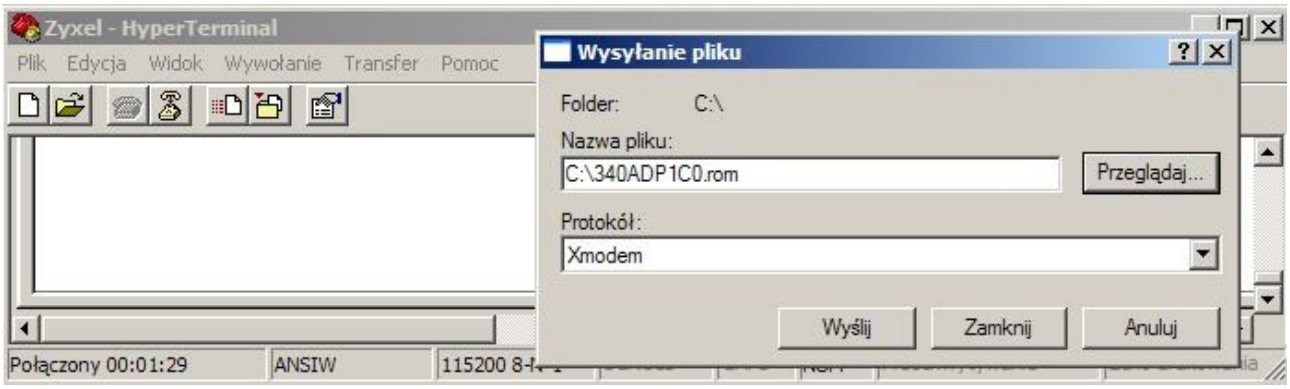


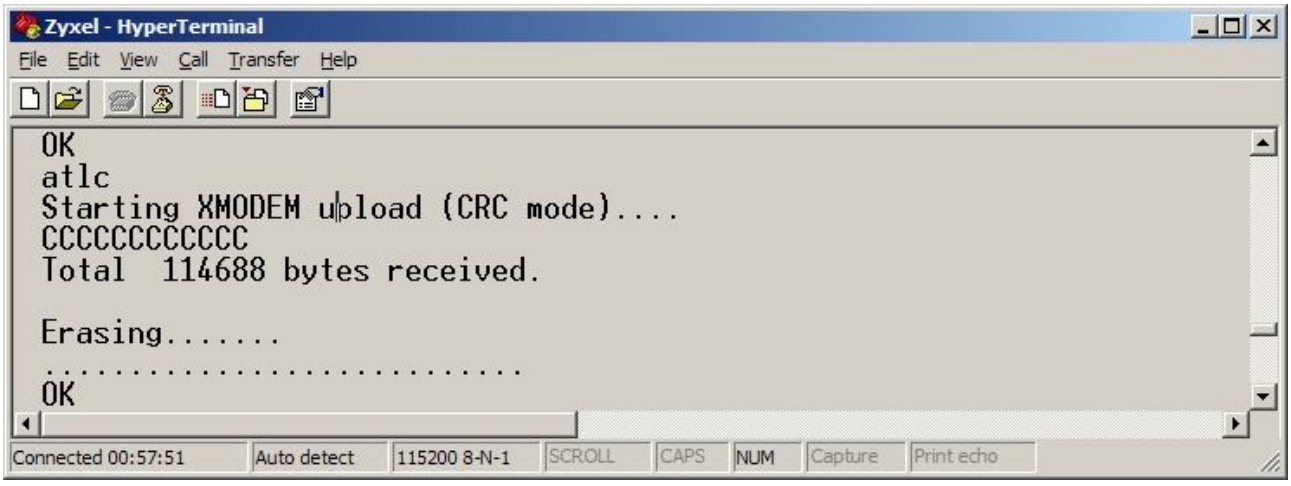


Po ponownym połączeniu możemy już przystąpić do wczytywania nowego FW: najpierw plik konfiguracyjny użytkownika (340ADP1C0.rom- krótszy z plików umieszczonych w archiwum), a następnie sam FW(340ADP1C0.bin)

ATLC
(upload router configuration file to flash ROM)

Router oczekuje teraz spokojnie na przesłanie pliku, wypluwając z siebie literki "C"...
Nie jest to nic niepokojącego, tak ma być . W menu Hyperterminala wybieramy Transfer>Wyślij plik i wskazujemy, gdzie znajduje się plik 340ADPC10.rom do wysłania. Jako protokół ustawiamy Xmodem i klikamy "Wyślij".

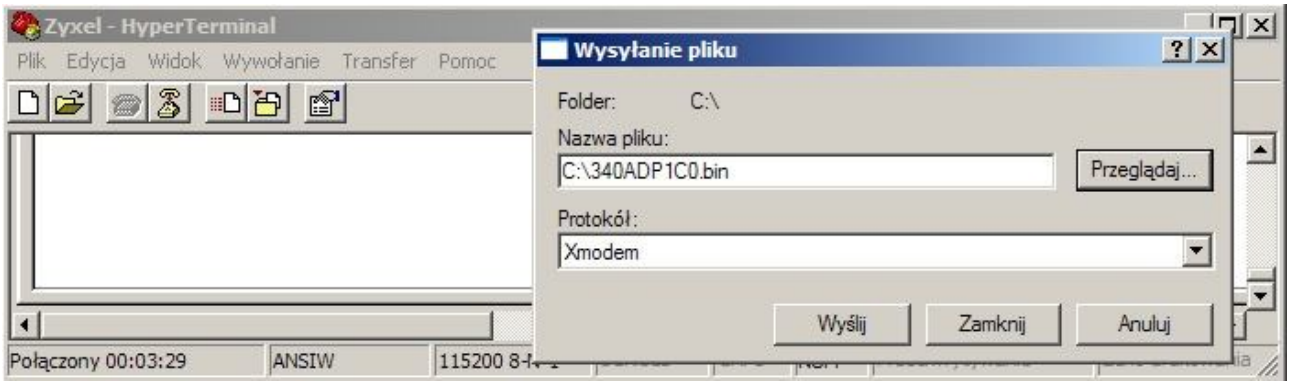


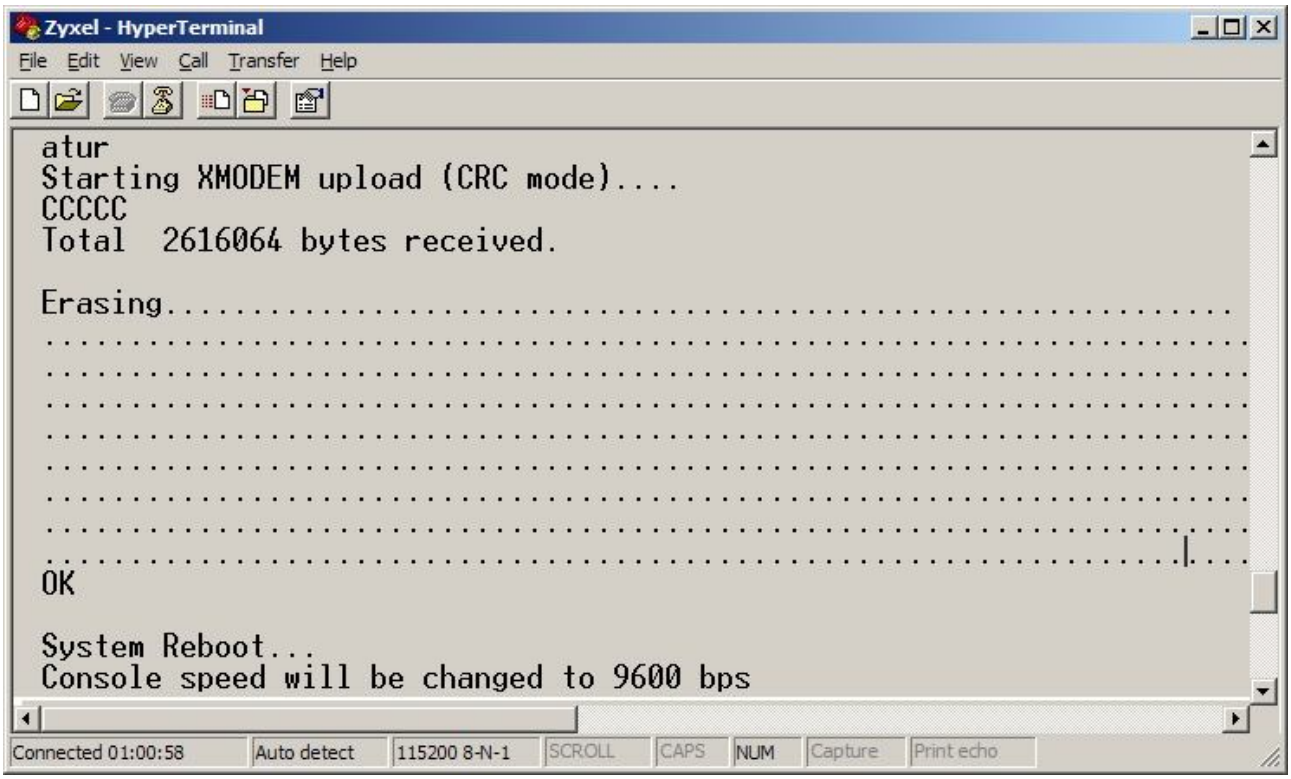


Po otrzymaniu komunikatu "OK" mamy już wczytany plik konfiguracyjny. Firmware ładujemy komendą :

ATUR
(upload router firmware to flash ROM)

Plik również wysyłamy poprzez Hyperterminal: Transfer>Wyślij plik i wskazujemy plik 340ADP1C0.bin do wysłania. Protokól Xmodem. Czekamy cierpliwie na komunikat "System reboot..." (wysyłanie przy tej prędkości konsoli może potrwać 5-6 minut)





To wszystko! Sprzęt ma już "generyczne" oprogramowanie ZyXEL-a, z odblokowanymi wszystkimi opcjami :)
Po reboocie router zgłosi się pod nowym adresem 192.168.1.1 , domyślne hasło : 1234

Podziękowania

Serdecznie dziękuję wszystkim, którzy swoją wiedzą przyczynili się do sukcesu w realizacji tego mini-projektu. W swojej pracy nad debrandingiem korzystałem z następujących źródeł:

Kolja Waschk - Running uCLinux on a ZyXEL router
http://www.ixo.de/info/zyxel_uclinux/

Stefan Kaiser - Anleitung zum Umflashen des
ARCOR-DSL WLAN-Modem 100 zum Original ZyXEL Prestige P660HW-67
http://www.stkaiser.de/anleitung/

Forum ADSL Ayuda
http://www.adslayuda.com/foro.html

Upload grupy newsowej Zyxel
http://www.jstic.com/Newsgroup/Zyxel/

Pozdrawiam i życzę powodzenia :) **Stefan Goryl** ®