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 <u>S.A.</u> 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 <u>dostosowany do pracy przy poziomach logicznych 0/3,3V</u> (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:

stawienia portu			
Liczba <u>b</u> itów na <mark>s</mark> ekundę:	9600	•	
Bity <u>d</u> anych:	8	•	
P <u>a</u> rzystość:	Brak	•	
Bity <u>s</u> topu:	1	•	
St <u>e</u> rowanie przepływem:	Brak	<u>-</u>	
		Przywróć domys	ślne
-			

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.

```
Zyxel - HyperTerminal
                                                                               - 0 ×
File Edit View Call Transfer Help
02 30 3
                                                                                   *
 Bootbase Version: V1.13 | 02/16/2006 14:05:00
 RAM: Size = 32768 Kbytes
 DRAM POST: Testing:
                           - OK
 Bootbase Version: V1.13 | 02/16/2006 14:05:00
RAM: Size = 32768 Kbytes
 DRAM POST: Testing: 32768K
 OK
 FLASH: AMD 32M *1
 ZvNOS Version: V3.40(ASU.1) | 04/21/2008
                                                    10:35:08
 Press any key to enter debug mode within 3 seconds.
4
                Auto detect
                          115200 8-N-1
                                           CAPS NUM Capture
                                                             Print echo
Connected 00:05:24
                                    SCROLL
```

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"

🏀 Zyxel - HyperTerminal	
<u>File Edit View Call Transfer Help</u>	
Enter Debug Mode	•
atsh	
ZyNOS Version : V3.40(ASU.1) 04/21/2008 10:35:08	
Bootbase Version : V1.13 02/16/2006 14:05:00	
Vendor Name : ZyXEL Communications Corp.	
Product Model : P-2602R-D1A	
ZyNOS ROM address : b0020000	
System lype : /	
MAC Address : 00 6	
Default Country Code : F6	
Boot Module Debug Flag : 00	
RomFile Version : 44	
RomFile Checksum : 55d8	
ZyNOS Checksum : c01e	
Core Checksum : 410/	
SNMP MIB_level & OID : 060102030405060708091011121314151617181920	1
Main Feature Bits : CO	
Other Feature Bits :	
00 00 00 00 00 00 00 00-01 41 13 00 00 00	
OK NO	
	· []
Connected 00:06:48 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print echo	

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)

🍓 Zyxel - HyperTerr	ninal							
<u>File Edit View Call</u>	<u>T</u> ransfer <u>H</u> elp							
	12 2							
aten1,8C43 OK	C295							11
4								
Connected 00:15:19	Auto detect	115200 8-N-1	SCROLL	CAPS	NUM	Capture	Print echo	1.

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)

🗞 Zyxel - HyperTerminal	X
Eile Edit View Call Transfer Help	
atdu 0x94003110,100 94003110: 00 00 00 00 00 00 00 00 00 00 00 00 5A 79 58 45 94003120: 4C 20 43 6F 6D 6D 75 6E-69 63 61 74 69 6F 6E 73 94003130: 20 43 6F 72 70 2E 00 00-00 00 00 00 50 2D 32 36 94003140: 30 32 52 4C 2D 44 31 41-00 00 00 00 00 00 00 00 00 00 94003150: 00 00 00 00 00 00 00 00 00 00 00 00 0	•
940031C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	J

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

🍖 Zyxel - HyperTerminal								
<u>File Edit View Call Transfer Help</u>								
atdu 0x94003164,2 94003164: 01 99							••	<u> </u>
OK atwb 0x94003164,9d								
atwb 0x94003165,17 0K								
atdu 0x94003164,2 94003164: 9D 17								-
•								
Connected 00:41:24 Auto detect	115200 8-N-1	SCROLL	CAPS	NUM	Capture	Print echo		1.

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

Ele Edt Yew Call Transfer Help Image: State	💑 Zyxel - HyperTerminal	×
ATBT1 OK atsb i.i. OK atbu ZyNOS Version : V3.40(ASU.1) 04/21/2008 10:35:08 Bootbase Version : V1.13 02/16/2006 14:05:00 Vendor Name : ZyXEL Communications Corp. Product Model : P-2602R-D1A ZyNOS ROM address : b0020000 System Type : 7 MAC Address : 00 Gefault Country Code : F6 Boot Module Debug Flag : 00 RomFile Checksum : c01e Core Checksum : 4107 SNMP MIB level & 0ID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : C0	Eile Edit View Call Transfer Help	
ATBT1 OK atsb OK atbu ZyNOS Version : V3.40(ASU.1) 04/21/2008 10:35:08 Bootbase Version : V1.13 02/16/2006 14:05:00 Vendor Name : ZyXEL Communications Corp. Product Model : P-2602R-D1A ZyNOS ROM address : b0020000 System Type : 7 MAC Address : 00 6 Default Country Code : F6 Boot Module Debug Flag : 00 RomFile Version : 44 RomFile Checksum : 55d8 ZyNOS Checksum : c01e Core Checksum : 4107 SNMP MIB level & 0ID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : C0		
Default Country Code : F6 Boot Module Debug Flag : 00 RomFile Version : 44 RomFile Checksum : 55d8 ZyNOS Checksum : c01e Core Checksum : 4107 SNMP MIB level & OID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : 00 0ther Feature Bits :	ATBT1 OK atsb ÖK atbu ZyNOS Version : V3.40(ASU.1) 04/21/2008 10:35:08 Bootbase Version : V1.13 02/16/2006 14:05:00 Vendor Name : ZyXEL Communications Corp. Product Model : P-2602R-D1A ZyNOS ROM address : b0020000 System Type : 7 MAC Address : 00 6	
RomFile Version : 44 RomFile Checksum : 55d8 ZyNOS Checksum : c01e Core Checksum : 4107 SNMP MIB level & OID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : 9D 17 00 00 00 00 00 00 00 00 00 00 00 00 00	Default Country Code : F6 Boot Module Debug Flag : 00	
RomFile Checksum : 55d8 ZyNOS Checksum : c01e Core Checksum : 4107 SNMP MIB level & OID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : 9D 17 00 00 00 00 00 00 00 00 00 00 00 00 00	RomFile Version : 44	
Zynos Checksum : Cole Core Checksum : 4107 SNMP MIB level & OID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : 9D 17 00 00 00 00 00 00 00 00 00 00 00 00 00	RomFile Checksum : 55d8	
SNMP MIB level & OID : 060102030405060708091011121314151617181920 Main Feature Bits : C0 Other Feature Bits : 90 17 00 00 00 00 00 00 00 00 00 00 00 00 00	Core Checksum : CULE	
Main Feature Bits : CO Other Feature Bits : 190 17 00 00 00 00 00 00 00 00 00 00 00 00 00	SNMP MIB level & OID : 060102030405060708091011121314151617181920	
Uther Feature Bits : 190 17 00 00 00 00 00 00 00 00 00 00 00 00 00	Main Feature Bits : CO	
	Uther Feature Bits :	
OK 🗾	OK	1

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)

🍓 Zyxel - HyperTerminal		_O×
<u>File E</u> dit <u>V</u> iew <u>C</u> all <u>T</u> ransfer <u>H</u> elp		
atba5		<u> </u>
Now, console speed w	ill be changed to 115200 bps	-
		-
		•
Connected 00:50:10 Auto detect	115200 8-N-1 SCROLL CAPS NUM Capture Print echo	

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

Zyxel - HyperTerminal	_[0]
Plik Edycja Widok Wywołanie Transfer Pomoc	
Czekaj na wywołanie	
Zakończ oczekiwanie	
Odłącz	
<u></u>	
(Þ
ozłącza z systemem zdalnym.	
Zyxel - HyperTerminal	
ik Edycja Widok Wywołanie Transfer Pomoc	
Nowe połączenie	
Zanisz	
Zapisz jako	
Davkui	
Właściwości	J
Zakończ Alt+F4	
łaściwości: Zyxel	🛛 🗙 Właściwości: COM1
Łączenie z Ustawienia)	Ustawienia portu
1	
Zyxel Zmień ikonę	
	Liczba bitów na 115200
	sekundę: In 19200
Kraj/region: Polska (48)	Bity danych:
Wprowadź numer kierunkowy bez prefiksu rozmowy	
zamiejscowej.	Parzuetość: Prok
Numer 42	
Numer telefonu:	Piturtenu: 1
Połącz używając: COM1	Sterowanie
Konfigura	przepływem: Brak
🔽 Użyj kodu kraju/regionu i numeru kierunkowego	Przywróć domyślne
Ponownie wybierz numer, jeśli zajęte	
OK Anuluj	OK Anuluj Zastosuj

🍓 Zyxel - HyperTer	minal			
Plik Edycja Widok	Wywołanie Transfer Pomoc			
	Wywołaj Czekaj na wywołanie Zakończ oczekiwanie			
	Odłącz			
Łączy z systemem zdalr	iym.			

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".

🌄 Zyxel - HyperTerminal	Wysyłanie pliku	
Pilk Edycja Widok Wywołanie Transfer Pomoc	Folder: C:\ Nazwa pliku:	
	C:\340ADP1C0.rom Protokół:	Przeglądaj
	Xmodem	
Połączony 00:01:29 ANSIW 115200 8-	Wyślij Z	amknij Anuluj ja

🍓 Zyxel - HyperTern	ninal							
<u>File Edit View Call</u>	<u>T</u> ransfer <u>H</u> elp							
D 🖻 🍙 🔏 💷	1 <u>7</u>							
OK								
atlc								
Starting X	40DEM ubl	oad (CRC	mode).					
000000000000000000000000000000000000000	00	•••••	•					
Total 1140	588 bytes	received						
Erasing								<u> </u>
OK								T
•								•
Connected 00:57:51	Auto detect	115200 8-N-1	SCROLL	CAPS	NUM	Capture	Printecho	

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)

Water Expertentional Plik Edycja Widok Wywołanie Transfer Pomoc	Wysyłanie pliku	·기× १×
	Folder: C:\ Nazwa pliku:	
	C:\340ADP1C0.bin	Przeglądaj
	Xmodem	•
	Wyślij Zamknij	Anuluj [
Połączony 00:03:29 ANSIW 115200 8-		ia //

🏀 Zyxel - HyperTerminal		۲
Eile Edit View Call Transfer Help		
atur Starting XMODEM upload (CRC mode) CCCCC Total 2616064 bytes received.		
Erasing		
ÔΚ	 	
System Reboot Console speed will be changed to 9600 bps		1
ا	•	1
Connected 01:00:58 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print echo		11.

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 miniprojektu. W swojej pracy nad debrandingiem korzystałem z następujących żródeł:

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 powodzienia :)