A month or so ago I bought a ZyXEL P-2602HWL-61C router on ebay, and was annoyed to find it had the custom TPG firmware on it, which I couldn't upgrade.

Not one to be daunted, I hit the net and found out lots of other ZyXEL models had been tweaked (mostly by people in Europe.) So the other night I got tweaking, and managed to convince my router to accept the standard firmware. I thought I'd post the steps to do it, as a lot of people have been asking about it.

DISCLAIMER

TPG don't lock the ZyXEL modem to their service (or sell it any more), so they will suffer no financial loss by it being reverted to the ZyXEL firmware. I'm not a TPG customer, so I have no use for the TPG firmware.

Also, doing this is not overly simple, and totally untested apart from my experience, and plenty of people have broken their routers playing with the debug console. It's a mega hack, which involves guessing/finding the address in RAM where a temporary buffer is allocated, and changing a byte in it. Therefore, I make no guarantees, and take no responsibility for anyone creating a doorstop.

Moreover, it does not seem possible to backup the old firmware from the router (I tried but the transfer kept failing) , so AFAIK there is no way to go back to the TPG firmware after you do this. If you're a TPG user, you may do best to stick with their version.

Finally, it seems like I had the old TPG firmware - V3.40(ADF.1) - and there is a newer TPG firmware which is newer than any other firmware (generic or not) that I've managed to find on the net.

CREDIT

I used a bunch of web pages to learn about the ZyXEL console, debug mode, etc. There's no way I could have done this without copying other people's techniques.

Lots of information (debug password, memory structure) came from this page:
www.ixo.de/info/zyxel_uclinux
(although that page is for a different router, running on different architecture.)

What you need

A serial cable (see below), and a serial port terminal emulator which can do XMODEM transfers (Hyperterminal will probably do fine.)

Step One: Build a cable

The ZyXEL has an internal serial port which you will use to communicate with it. The port is an inline header, same size as a CD-Audio cable:

1 - GND
- (No pin)
2 - TX
3 - RX
4 - (Pin, not used

The port needs a 3.3v-level serial interface to function. I used a Siemens C55 mobile cable I bought on ebay for $10 (shipped), and a CD Audio cable I had lying around.

Here's a web page (in German) about building one of these cables (includes diagrams.)
www.stkaiser.de/anleitun...usb_unboxed.html

My approach was slightly different. That page connects the CD Audio cable to the USB end of the mobile phone cable. I connected the cable at the Siemens plug end, so it would be longer. Here's the Siemens pinout:
pinouts.ru/CellularPhone...c55_pinout.shtml

The connections I used were as follows:

Siemens End -> ZyXEL End
Pin 2 -> Pin 1
Pin 3 -> Pin 3
Pin 4 -> Pin 2

Step Two: Boot console

Connect the serial cable, and configure a terminal emulation program for 9600bps with 8,N,1 and no flow control of any kind. It's vaguely possible the default terminal speed has been changed (you can look it up in the router settings via telnet.)

Plug in your cable, and turn on the router. Data should begin appearing immediately. If you don't see anything, something is wrong with your cable.

Bootup looks like this:

Bootbase Version: V1.09 | 07/29/2004 16:00:00
RAM: Size = 32768 Kbytes
DRAM POST: Testing: 32768K
OK
FLASH: AMD 32M *1

ZyNOS Version: V3.40(ADF.1) | 07/12/2005 18:00:00

Press any key to enter debug mode within 3 seconds.
.....

Press a key when prompted, and you'll drop into the debug console.

NOTE: If your ZyNOS version and/or BootBase Version are different to those shown, you have a different firmware. Take care when following the rest of these directions, because things may be different.

Step Three : Debug Mode

Type "AT<CR>" and you should see the response "OK". All the commands take this form.

NOTE: You can use the ATHE command to see all the available debug commands, I won't bother listing them here. Lots of useful info for those who are curious is available at www.ixo.de/info/zyxel_uclinux

Step Four : Show hardware/manufacturer info from Flash

type ATSH<CR>

```
ATSH
ZyNOS Version : V3.40(ADF.1) | 07/12/2005 18:00:00
Bootbase Version : V1.09 | 07/29/2004 16:00:00
Vendor Name : ZyXEL Communications Corp.
Product Model : Prestige 2602HWL-61C
ZyNOS ROM address : b0020000
System Type : 7
MAC Address : 0013494B3DDA
Default Country Code : F4
Boot Module Debug Flag : 00
RomFile Version : B7
RomFile Checksum : f3a3
ZyNOS Checksum : 4d10
Core Checksum : 7d23
SNMP MIB level & OID : 060102030405060708091011121314151617181920
Main Feature Bits : C0
Other Feature Bits :
9D 14 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-01 41 13 00 00 00l
```

The "other feature bits" section at the bottom is what we need to change in order to unlock the router (specifically, the second byte - 14.)

Check that the rest of your details look vaguely similar to these, as well.

Step Five - Enable debug mode.

The password for debug mode is based on the router's MAC address. Look at the last digit of the router's MAC Address, shown in the output of the previous command. Mine was 'A'

Now find the corresponding password:

Last Digit Password
...0 or ...8 10F0A563
...1 or ...9 887852B1
...2 or ...A C43C2958
...3 or ...B 621E14AC
...4 or ...C 310F0A56
...5 or ...D 1887852B
...6 or ...E 8C43C295
...7 or ... F C621E14A

Enter the following command:

```
ATEN1,<PASSWORD>
```

... you are now in "debug" mode.

Step Six - Create working buffer

The router has a "working buffer" copy of the "hardware info" table you saw above. Execute the following commands to set up and show the working buffer:

```
ATCL

ATCB

ATBU
```

.. the output (buffer contents) should look the same as the ATSH output, above.

Step Seven - Find buffer location in RAM

Execute this command:

```
ATDU 0x94003110,2
```

The output should look like this:

94003110: 9D 14

IF THE OUTPUT DOES NOT MATCH THE FIRST TWO FEATURE BITS: STOP NOW!! Different output means that your working buffer is resident at a different location in memory, and if you continue then you will probably break your router. You

will need to use the ATDU and/or ATDO commands to dump memory in this area until you see a string of bytes which look like the "Feature Bits" in the ATBU output. In the more recent F/Ws, it seems to load at around 0x94003118.

Step Eight - Change feature bits in working buffer

Assuming the output matches, you need to change that "14" to an "0A". Execute the following command:

```
ATWB 0x94003111,0A
```

Then run '`ATBU`' and check that the first two feature bits have changed to "9D 0A".

If anything else appears, turn your router off and back on to clear the RAM.

Step Nine: Save Working Buffer Back to Flash:

Execute the following commands to write the working buffer back to flash memory:

```
ATBT1
```

```
ATSB
```

... now the output of ATSH should look the same as ATBU. If it does, you've done it - the router is now a "generic model"!!

Step Ten: (Optional) Increase Transfer Speed

If you want, run the command `ATBA5` to change the serial port speed to 115200bps. You will need to modify your terminal program to suit.

Step Eleven: Upload the new configuration file and firmware

The existing firmware will no longer work because the router is now a different "model", so you need to upload some new generic model firmware.

First, upload the .ROM configuration file from the firmware. Type

```
ATLC
```

... then use XMODEM to transmit 340mv4c0.rom (or similar.) The router should accept the file.

Second, upload the actual firmware file. Type

```
ATUR
```

... then use XMODEM to transmit 340mv4c0.bin (or similar.) The router should accept the firmware, output some info, and then automatically reboot.

If you see gibberish at the serial port after this point, you need to reset your console speed to 9600bps.

Congratulations, you now have an unlocked ZyXEL 2602HWL-61C!