



www.CABLES ZYXEL.es.kz  
OPTIMIZA TU ROUTER AL MÁXIMO

[HOME](#) :: [MANUAL](#) :: [CREA TU CABLE](#) :: [PEDIDOS](#) :: [FORO](#) ::

## MANUAL PASO A PASO Prestige 660HW-D1



Manual Paso a Paso para cambiar el firmware original de los routers comprados a telefonica al firmware original Zyxel con muchas mas ventajas y prestaciones.

A tener en cuenta 3 cosas:

- Al realizar el pase de firmware telefonica a Zyxel perderemos toda la configuración de acceso a internet, por tanto tened a mano la hoja de datos de telefonica y o anotad vuestra configuracion actual, ips de acceso, dns, etc. para la posterior reconfiguracion del router.
- Los usuarios que tengan contratado Imagenio es posible que no les funcione con el firmware oficial, aunque siempre estas a tiempo de volver a ponerle el firmware de telefónica.
- Colocar y modificar la Bootbase no es dificil pero es delicado, os recomiendo encarecidamente que primero leais todos los pasos, y despues seguidlos sin saltaros nada. Al subir la bootbase con un corte de alimentacion o modificarla mal significa router KO. Si se tiene alguna duda consultad los [foros de adslayuda](#), donde estan Piolinsy y otros foreros activamente dispuestos a resolver cualquier duda.

---

### PASO 1

Antes de nada vamos a descargar todos los programas necesarios:

- [TeraTerm Pro](#)
- [ZynPass1.2\\*](#) o entra en [ZynPass JS v.0.1.4a](#)
- [Firmware AGL\\_1 Zyxel](#) (3.10.06) o [Firmware AGL\\_4 Zyxel](#) (27.02.07)
- 1 Editor Hexadecimal cualquiera del tipo winhex, hex workshop, ultraedit 32, podeis descargaros el que mas os guste [aqui](#)

\*Es posible que no te funcione este programa si no tienes instaladas las extensiones .NET Framework de microsoft. Se consiguen en windows update.

---

### PASO 2

Procedemos a abrir el router:

- Desenchufamos el router
- Desencajamos la carcasa superior.
- Una vez abierto tened cuidado de no meter nada metalico, que pudiera cortocircuitar algo, y evitar hacer contacto con los dedos, podeis dañar algunos circuitos con vuestra electricidad estática.

Cuidados del circuito/cable:

- Manipular con cuidado y no pegar tirones.
- No colocar sobre una superficie metálica, ya que se cortocircuitaría todo.

PASO 3

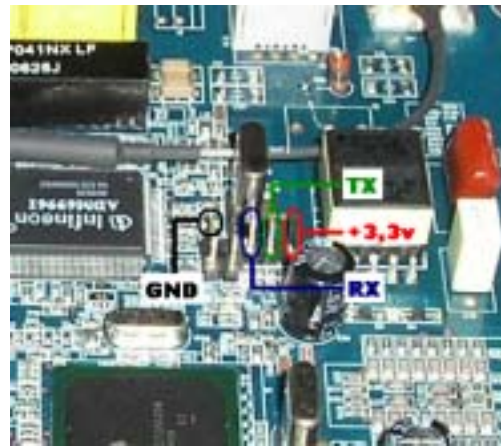
Especial atención en este punto. Vamos a conectar el circuito/cable serie del pc al router.



El conector gris del cable serie suministrado tiene 6 agujeritos, aunque solo se usan 4 cables, esto puede ocasionar que nos equivoquemos facilmente de posicion al conectarlo por tanto VIGILAD.

En el router vemos un conector base de 4 puas, pues bien con el **router apagado** colocamos el **cable marron (-)** en el extremo solitario izquierdo donde pone GND en la foto.

Imagen donde conectar el cable del modelo blanco:



Imagenes en profundidad pertenecientes al modelo negro:



Ya solo nos queda conectar el otro extremo del circuito en el puerto serie del PC, en caso de haber mas de 1, escogeriamos el COM1:



#### PASO 4

Ahora que ya tenemos el cableado conectado procederemos a utilizar el TeraTerm Pro para cargar nuestro nuevo firmware. Este modelo es algo mas complicado que su hermano negro porque hay que modificarle la bootbase mediante un editor hexadecimal, pero si seguís todos los pasos del manual al pie de la letra no tendréis problemas.

Tomad nota del manual desarrollado por Piolinso de [ADSLAYUDA](#) que se describe a continuación:

Para evitar problemas de compatibilidad con algún cable de comunicación es recomendable subir la velocidad de comunicación del puerto de serie interno del router a través de telnet..para eso necesitamos conocer la IP del router (puerta de enlace) que por defecto suele ser 192.168.1.1, una vez que la tengamos anotada, nos iremos al menú inicio--->ejecutar--->cmd y pondremos esto:

#### Código:

```
Telnet xxx.xxx.xxx.xxx <----- Esto sera la puerta de enlace
```

Una vez conectados nos pedirá el password (por defecto 1234), lo introducimos y pulsamos intro...luego entraremos en el menú 24 System Maintenance--->2.System information and console port speed--->2.console port speed para cambiar la velocidad por defecto (que viene a ser 9600bps) lo haremos con la barra espaciadora hasta que nos muestre la que deseamos..en mi caso lo he dejado prefijada en 115200bps, para terminar pulsamos intro para guardar los cambios.

Bien, ahora es el momento de entrar en modo debug extendido a través del cable y el programa TeraTerm Pro que habeis descargado antes.

Una vez ejecutado, seleccionamos la velocidad de comunicación y puerto adecuado (en este caso sería com1 a 115200bps) tal como se muestra en la imagen:



Ahora procederemos a encender el router y entraremos en modo debug, para ello hay que pulsar una tecla mientras el router está en espera (nos aparecerán unos puntitos)

Llegados a este punto es necesario habilitar los comandos que nos permitan hacer lo que pretendemos así que tendremos que habilitar el modo debug extendido..el proceso sería el siguiente:

Introducir a través del TeraTerm los siguientes comandos:

**Código:**

```
ATSE
0017829D229F <----- Esta es la semilla, cambia cada vez que se teclea ATSE
OK
```

Con esa semilla hay que calcular el password con el programa [ZynPass1.2](#)

Una vez calculado el password (en mi caso CA21F6FB) se introduce con el comando:

**Código:**

```
ATEN1,CA21F6FB <----- Sustituir CA21F6FB por el password en cada caso
OK <----- Todo OK
```

Con esto habremos conseguido que sean operativos todos los comandos (incluso los peligrosos)

Pues bien sabiendo que telefónica ha capado la posibilidad de cambiar los feature bits directamente con el comando

**Código:**

**ATFE**

lo que vamos a hacer es engañar al router para que acepte el comentado cambio de los feature bits sin rechistar...como? pues otra vez es algo relativamente sencillo...pero primero un poco de teoría:

**Piolinso escribió:**

Respecto a lo de la bootbase y la .rom, vamos a ir por partes...

La .rom que viene habitualmente en los .zip de los firmwares de zyxel, es un archivo que alberga en su interior la configuración de fábrica del router, entiéndase por configuración a todos los parámetros que se podrían modificar vía web o telnet..

Luego está la bootbase que es el bootloader que utilizan los routers de zyxel, digamos que es como una especie de bios que se encarga de arrancar el router, hacer los test de encendido y si el firmware es correcto pasar a ejecutarlo...la bootbase viene el formato .bm y se puede subir siguiendo las instrucciones del manual que elaboré en su día...este es el link para descargar el manual detallado de como hacer un backup o dump y subirle la bootbase

[ManualBootbase1.06.pdf](#)

Ok, pues la idea para saltarse esa medida de seguridad que nos impide modificar los feature bits es hacer un volcado de la bootbase del D1 y modificarle los feature bits 0 y 1 por los adecuados y subírsela de nuevo...todo el proceso se describe en el manual de actualización de la bootbase en PDF mencionado unas líneas mas arriba, aunque para facilitar las cosas hago un resumen de lo mas reseñable aquí:

Lo primero que vamos a hacer es obtener una copia de seguridad de nuestra bootbase original por si la necesitáramos en el futuro, para ello utilizaremos el comando:

**Código:**

**ATDO b0000000,4000**

que nos mostrará en el teraterm lo de

**Código:**

Starting XMODEM download (CRC mode).....

En este momento debemos de recibir el archivo y darle un nombre seleccionando:

File--->Transfer--->Xmodem--->Receive.... ponéis el nombre que queráis y OK

Para editar la bootbase necesitaremos un editor hexadecimal tipo winhex, hex workshop, ultraedit 32... teneis un enlace arriba donde descargarlo.

Ahora con el editor hex preferido tenéis que abrir el dump de vuestra bootbase y bajar hasta el final del archivo, con lo cual nos mostrará algo parecido a esto:

```
00003FD0 | B0 01 00 00 00 00 07 00  BA 23 00 00 00 00 00 00 | *      |#
00003FE0 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |
00003FF0 | 02 41 13 00 00 00 C0 00  22 22 22 22 22 22 FF 01 | A      |A *****y|
```

Llegados a este punto lo que tenemos que hacer es modificar los feature bits que se encuentran en la dirección off-set 3FD8 y 3FD9 por los que pertenecen al firmware oficial del zyxel 660HW-D1, de manera que los other feature bits quedarían tal y como se muestra en el recuadro rojo de la imagen superior

En la bootbase además se encuentran descritos los datos del fabricante, nombre del producto, dirección mac..y alguna que otra cosa adicional...este es un resumen de su contenido respecto a esos feature bits..

**Código:**

```
00003F90 VVVV VVVV VVVV VVVV VVVV VVVV VVVV VVVV ZyXEL Communicat
00003FA0 VVVV VVVV VVVV VVVV VVVV VVVV VVVV VVVV ions Corp.....
00003FB0 PPPP PPPP PPPP PPPP PPPP PPPP PPPP Prestige 660HW-X
00003FC0 PPPP PPPP PPPP PPPP PPPP PPPP PPPP X.....
00003FD0 ZZZZ ZZZZ ???? TT?? FFFF FFFF FFFF FFFF .....
00003FE0 FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF .....
```

00003FF0 FFFF FFFF FFFF BB?? MMMM MMMM MMMM CCDD .....

S = SNMP MIB level & OID  
 V = Vendor Name  
 P = Product Model  
 Z = ZyNOS Rom Address  
 T = System Type  
 F = Other Feature Bits  
 B = Main Feature Bits  
 M = MAC Address  
 C = Default Country Code  
 D = Boot Module Debug Flag (00 disable, 01 enable)

Si no queréis volver a calcular el password y semilla y entrar directamente en modo debug extendido solamente hay que modificar el valor de DD que se encuentra en la posición 3FFF por un 01 (originalmente está a 00)

Bueno, pues una vez modificada la bootbase, para subirla a vuestro router se pueden volver a seguir los pasos del comentado PDF que si los resumimos:

Primero deberemos introducir este comando

**Código:**

**ATBT1**

para que nos permita escribir en el bloque 0 y después utilizar este otro comando

**Código:**

**ATUX0**

que significa:

**Código:**

ATUXx(y) xmodem upload from flash block x to y

Llegados a este paso nos mostrara el TeraTerm lo de

**Código:**

Starting XMODEM upload (CRC mode).....

en este momento ya podemos subirle la bootbase editada con los feature bits modificados para el firmware oficial seleccionando en el Teraterm File--->Transfer--->Xmodem--->Send

Una vez finalizado el proceso el TeraTerm debería de mostrarnos lo siguiente:

**Código:**

ATBT1  
 ATUX0  
 Starting XMODEM upload (CRC mode).....  
 C  
 Total 16384 bytes received.  
 Erasing.  
 ....  
 OK

Pues con este sencillo proceso hemos conseguido subirle la bootbase de nuestro zyxel ya modificada de forma que el router acepte sin quejarse el firmware oficial...

Ahora sería el momento de proceder a subirle el Firmware del Zyxel 660HW-D1 Oficial P-660HW-D1\_V3.40(AGL.1)C0\_Standard (.bin), este firmware nos lo podremos descargar por ejemplo desde aquí:

[ftp://ftp.zyxel.com/P-660HW-D1/firmware\\_...\\_L.1\)C0.zip](ftp://ftp.zyxel.com/P-660HW-D1/firmware_..._L.1)C0.zip)

Posteriormente después de descomprimirlo en el directorio deseado emplearemos el comando

**Código:**

**ATUR**

que nos volverá a decir lo de

**Código:**

Starting XMODEM upload (CRC mode).....

con lo que le subiremos el Firmware AGL.1 (340AGL1C0.bin) seleccionando en el TeraTerm: File--->Transfer--->Xmodem--->Send , tal como figura en la imagen:



