

# AVERIGUAR EL PASSWORD DE CONSOLA MODEM/ROUTER 3COM 812

## (Método Harkonen simplificado)

El procedimiento que se explica a continuación nos permitirá averiguar el password de consola desconocido en un módem/router 3Com OfficeConnect 812.

Este procedimiento es una simplificación del método que en su día reveló **Harkonen** en la Web de Bandaancha (<http://www.bandaancha.st/weblogart.php?artid=1305>) y presenta, respecto al procedimiento original de Harkonen, la ventaja de no tener que desoldar la patilla nº 4 del chip de la EEPROM, con la mejora que ello representa en cuanto a la conservación de la integridad de dicho chip y, por ende, del módem/router y también la considerable menor dificultad en realizarlo.

A continuación explicaremos el método paso a paso.

## PRIMER PASO (PREPARACIÓN DEL ROUTER)

Empezaremos sacando la tapa al módem/router. Para ello nos ayudaremos de un destornillador de punta plana de tamaño mediano.

La tapa va fijada únicamente a presión, mediant lengüetas.

Con ayuda del destornillador, separaremos las lengüetas, procurando no forzarlas, al mismo tiempo que con los dedos iremos empujando la tapa hasta sacarla de su alojamiento.

## SEGUNDO PASO (COMUNICACIÓN MÓDEM/ROUTER-ORDENADOR)

Una vez extraída la tapa, procederemos a conectar el módem/router tanto a la alimentación eléctrica (a través de su alimentador), como al ordenador, mediante el correspondiente cable serie que conectaremos por uno de sus extremos en la parte trasera del módem/router al conector etiquetado como "Console" y por el otro extremo lo conectaremos a un puerto serie del ordenador (COM1 o COM2).

Deberemos asegurarnos de que existe comunicación módem/router → Ordenador a través del cable serie. Para ello, configuraremos el programa emulador de terminal que tengamos instalado en el ordenador, que puede ser el Hyperterminal si usamos Windows o el Minicom si usamos Linux, con los siguientes parámetros:

Bits por segundo: 9600

Bits de datos: 8

Paridad: Ninguna

Bits de parada: 1

Control de flujo: Ninguno

Luego, le damos alimentación al módem/router para comprobar que existe comunicación entre el mismo y el ordenador; lo cual nos vendrá indicado en el programa emulador de terminal si nos muestra la secuencia de arranque típica del módem/router.

## TERCER PASO (PROCEDIMIENTO PROPIAMENTE DICHO)

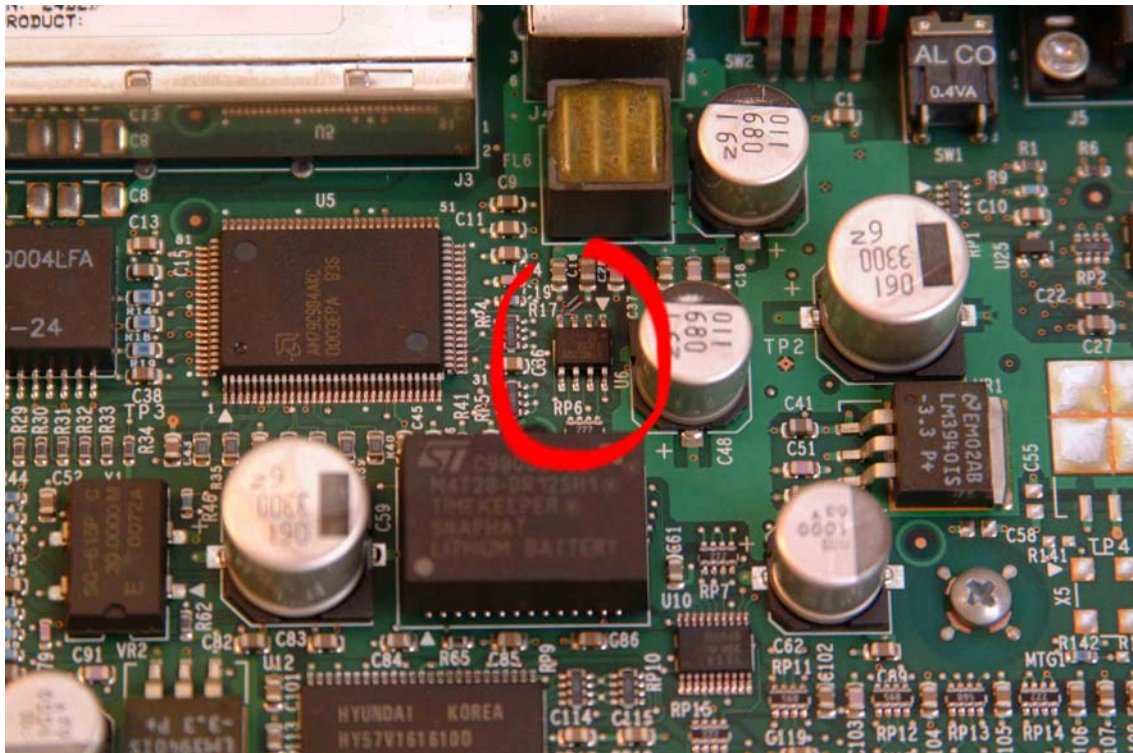
Este tercer paso lo dividiremos, a su vez, en varios apartados en aras a una mayor claridad:

**1.** Iniciaremos el proceso con el módem/router desconectado de la alimentación y conectado al ordenador con el cable serie indicado anteriormente.

2. Nos haremos con un trocito de cable conductor (de unos 30 mm de longitud) y de pequeña sección, al que, previamente, habremos pelado los extremos. Este cable nos servirá para establecer un puente entre las patillas nº 4 y nº 8 del chip de la EEPROM (cortocircuitarlas).

3. Localizaremos el chip de la EEPROM (marca ATMEL modelo 93C66 o equivalente), que viene etiquetado en la placa de circuito impreso como U6 o U23.

En la fotografía que se expone a continuación, vemos donde está ubicada la EEPROM (dentro del círculo rojo), así como su patilla nº 4 (señalada con una flechita y situada en la hilera superior, extremo izquierdo del chip visto desde arriba)



4. Usando el trocito de hilo conductor, que hemos citado anteriormente, haremos un “puente” entre las patillas nº 4 y nº 8 de la EEPROM (las mantendremos en contacto).

Para facilitar la localización de las patillas 4 y 8, veamos su posición en el siguiente esquema (chip visto desde arriba, en la misma posición que se observa en la fotografía):

4 3 2 1  
5 6 7 8

La patilla nº 1 es fácilmente reconocible porque viene marcada con un circulito y, además, está indicada también por un triangulito que apunta hacia ella y que está grabado en el propio circuito impreso.

5. Ejecutamos el programa emulador de terminal (Hyperterminal o Minicom) con los parámetros que hemos citado en el SEGUNDO PASO y luego procedemos a dar alimentación eléctrica al módem/router.

6. Seguiremos manteniendo el puente entre las patillas 4 y 8 de la EEPROM.

Cuando, en la secuencia de arranque del módem/router en el programa emulador de terminal, se llegue a la pregunta:

**Maintenance?**

deberemos pulsar la secuencia de teclas **CONTROL + B**, lo cual hará que entremos en el menú de Mantenimiento del módem/router **SIN QUE NOS PIDA CONTRASEÑA**.

Pulsaremos la tecla **INTRO**

**7.** Nos aparecerá la primera pantalla del Menú de Mantenimiento:

```
*** 3Com OfficeConnect Remote 812 - Maintenance Program ***
```

Top Level:

- 1) Diagnostics
- 2) Utilities
- 3) Restart System
- ?

Elegimos la opción **2) Utilities**

**8.** Aparecerá una segunda pantalla del Menú de Mantenimiento:

```
*** 3Com OfficeConnect Remote 812 - Maintenance Program ***
```

Utilities:

- 1) FLASH File/Disk Utilities
- 2) EEPROM Utilities
- 3) Memory Utilities
- 4) Other Utilities
- 5) Restart System
- 6) Return to Top Level Menu
- ?

Elegimos la opción **2) EEPROM Utilities**

**9.** Aparecerá la siguiente pantalla del Menú de Mantenimiento:

```
*** 3Com OfficeConnect Remote 812 - Maintenance Program ***
```

EEPROM Utilities:

- 1) Display EEPROM
- 2) Display MAC Address
- 3) Display Serial Number
- 4) Return to Utilities Menu
- ?

**MUY IMPORTANTE:**

**EN ESTE PUNTO, HAY QUE DESHACER EL PUENTE ENTRE LAS PATILLAS 4 Y 8.**

Luego, eliges la opción **1) Display EEPROM**

**10.** Nos saldrá en pantalla el volcado de la EEPROM. Algo parecido a esto:

```
000: 48 4C 59 32 31 31 31 41 32 33 37 38 00 00 00 00
010: 00 04 76 1A 23 78 FF 0B FF FF FF FF FF FF FF
020: FF A1 02 00 90 85 90 85 94 00 94 84 FF FF FF FF
030: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
040: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
050: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
060: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
070: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
0B0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0C0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0D0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0E0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0F0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
Press any key to continue...
```

La posición 0x23 indica con un **00** que está activado el password de consola. Si no estuviera activado lo indicaría con **FF**.

El password está contenido desde la posición 0x24 hasta que se encuentra el primer 00 o bien se completan 8 caracteres.

En el ejemplo de volcado que he puesto, el password es:

**90 85 90 85 94**

(remarcado en negrilla y color rojo)

## 11. DESCIFRADO DEL PASSWORD

Ahora deberemos pasar este password cifrado a texto, para ello, daremos estos tres pasos:

1. Emplearemos, por ejemplo, la calculadora de Windows en modo científico, marcaremos la opción "**Hex**" y escribiremos el primer número de la secuencia del password (en nuestro caso sería 90) y luego marcaremos la opción "**Dec**" para pasar dicho número a decimal.

En nuestro ejemplo, tendríamos:

90 85 90 85 94 → 144 133 144 133 148

2. Ahora debemos restar **32** a cada uno de los números.

En nuestro ejemplo, se convertiría en:

112 101 112 101 116

3. Finalmente, podemos, por ejemplo, empleando el Bloc de Notas de Windows pasar estos números a texto.

Esto lo lograremos, dentro de la aplicación Bloc de Notas, pulsando la tecla **Alt + el número**, es decir que, en nuestro ejemplo, tendríamos:

Alt+112 = **p**

Alt+101 = **e**

Alt+112 = **p**

Alt+101 = **e**

Alt+116 = **t**

Obtenemos el password de consola **pepet**

---

### Notas:

El autor de la fotografía (estupenda, por cierto) es el conocido **Antonio Martos**, desde aquí mi agradecimiento por la misma.

Añado también que todo el mérito de este procedimiento hay que atribuirlo al citado **Harkonen** y a un posteante anónimo de habla inglesa en el foro de Bandaancha, que son quienes han hecho los "deberes", habiéndome limitado yo a "pasarlos a limpio" con el único afán de facilitar las cosas al usuario que tenga el problema de desconocer el password de su módem/router.

**Tatolino 19/7/2003**