Tema 2: Configuración básica del sistema. La BIOS

1. Introducción

La ROM BIOS (o simplemente BIOS) está formada por un conjunto de programas que residen en una memoria no volátil en la placa base de un PC.

Los chips ROM BIOS actuales emplean un tipo de memoria EEPROM denominada *flash*. Se trata de memorias no volátiles (no pierden la información cuando desaparece la alimentación) que pueden leerse y borrarse eléctricamente de forma simple.

Los fabricantes de placas base no suelen escribir sus ROM BIOS. Compran chips de ROM BIOS a fabricantes especializados como Phoenix y AMI que los adaptan a cada placa base.

La ROM BIOS proporciona la siguiente funcionalidad:

- Un conjunto de rutinas básicas de E/S.
- Un programa de configuración de bajo nivel.
- Un conjunto de rutinas de detección, comprobación y configuración del hardware, denominado POST.
- Un cargador del sistema operativo.

En teoría, la ROM BIOS proporciona un conjunto de rutinas básicas de E/S, de ahí el nombre de Basic Input/Output System (BIOS), que son llamadas desde el sistema operativo a través de sus controladores (*drivers*) para acceder al hardware. Sin embargo, en la práctica, la mayor parte de los servicios de la ROM BIOS se emplean exclusivamente durante el inicio del sistema, hasta que se cargan los componentes básicos del sistema operativo, momento a partir del cual se utilizan las rutinas del propio sistema operativo.

2. Chip RTC/NVRAM

La ROM BIOS incorpora un programa de configuración (*setup*) que permite modificar información de configuración básica de los dispositivos de la placa base.

La información de configuración se almacena en un chip que hace las veces de reloj del sistema (mantiene la fecha y la hora) y que internamente incorpora además una pequeña memoria RAM. Este chip se denomina RTC/NVRAM (*Real-Time Clock and Non-Volatile RAM*). Tanto la fecha y hora como la información almacenada en la RAM no se pierde cuando se apaga el PC, pues el chip está alimentado por una pila.

El chip está hecho con tecnología CMOS que consume muy poca energía y permite que la pila dure varios años.

En la actualidad, el chip RTC/NVRAM suele estar integrado dentro de otro chip denominado Super I/O.

3. POST

La ROM BIOS incluye un conjunto de rutinas de detección, comprobación y configuración de hardware, denominadas POST (*Power On Self Test*). El POST se ejecuta nada más arrancar el PC y finaliza cuando comienza la carga del sistema operativo en memoria. Durante la ejecución del POST, pulsando una determinada tecla (típicamente la tecla F2 o Supr), se accede a la utilidad de configuración de la BIOS.

Hay tarjetas de expansión que incorporan sus propias ROM BIOS. Habitualmente se trata de tarjetas desde las que se puede cargar el sistema operativo. Por ejemplo, una tarjeta controladora SCSI, pinchada en una ranura PCI, incorpora una ROM BIOS que proporciona servicios de acceso a dispositivos SCSI, un programa de *setup* específico, y un POST específico que detecta y configura dispositivos SCSI.

4. Secuencia de arranque de un PC

Durante el arranque se ejecuta el código almacenado en la ROM BIOS de la placa base y en la ROM BIOS de tarjetas de expansión. Cuando el sistema arranca de nuevo tras una operación de reinicio, buena parte de las comprobaciones del POST no se llevan a cabo, acelerando el proceso de arranque.

A continuación se muestra la secuencia de operaciones que ocurren desde que se enciende el PC, hasta que comienza la carga del sistema operativo:

1. Cuando se pulsa el botón de encendido, la fuente de alimentación activa la señal PWR_OK. La placa base desactiva la señal de reset de la CPU y ésta comienza la ejecución.
2. La CPU arranca en modo real (direcciones de 20 bits, sin segmentación ni paginación). La primera instrucción que ejecuta es la que se encuentra en la dirección FFFFoh, incluida dentro de la ROM BIOS de la placa base. Esta instrucción salta a la primera instrucción del POST.
3. Durante el POST se ejecutan una serie de rutinas de detección, comprobación y configuración básica de los dispositivos clave del computador. Algunas rutinas muestran información de dispositivos por pantalla, otras incluso solicitan opciones al usuario, como la selección del dispositivo de arranque.
4. Casi al final del POST se buscan ROM BIOS adicionales presentes en tarjetas de expansión. Si se encuentra alguna de ellas y es válida, se le cede el control, pasando a ejecutarse el POST particular de la tarjeta. Si el arranque del sistema operativo no se lleva a cabo desde la tarjeta de expansión, ésta devuelve el control al POST de la ROM BIOS del sistema.
5. La ROM BIOS del sistema comprueba la pulsación de la tecla Supr que inicia la ejecución de la utilidad de configuración del sistema. Esta utilidad muestra los parámetros actuales del sistema, almacenados en el chip RTC/NVRAM. Estos parámetros, una modificados vuelven a almacenarse en el chip RTC/NVRAM.

6. De entre una lista de dispositivos con capacidad de proporcionar el sistema operativo se busca el primero que contenga un registro de arranque maestro válido (*Master Boot Record* o MBR).
7. Si se encuentra un MBR válido se carga en memoria el sector de arranque del sistema operativo, cuya dirección indica el MBR y se le cede el control del PC.
8. El sector de arranque del sistema operativo carga en memoria el núcleo del sistema operativo.

Las operaciones 2, 3, 4, 5, 6 y 7 las ejecuta el POST (código ROM BIOS). La operación 8 la ejecuta código del sistema operativo.

5. Errores del POST

Algunas de las rutinas del POST llevan a cabo comprobaciones sobre el hardware y pueden dar lugar a dos tipos de errores:

- Errores recuperables. No impiden el arranque del sistema pero deben ser tenidos en cuenta por el usuario. Ej.: Cuando el POST localiza un error de *checksum* en la ROM BIOS de una tarjeta de expansión, genera un mensaje de error.
- Errores terminales. Se tratan de errores graves que impiden el arranque del sistema. En ese caso, la ROM BIOS típicamente:
  - Envía una cierta secuencia de pitidos al altavoz.
  - El código de la rutina de comprobación se envía al puerto 80h de E/S.
  - Se intenta inicializar el vídeo y se escribe en la pantalla el código de la rutina de comprobación.

Además, al comienzo de cada rutina del POST, la BIOS escribe un código en el puerto 80h que identifica la rutina. Esto es útil cuando el sistema se cuelga en el POST, pues permite saber cual es la última rutina del POST que ha intentado ejecutarse.

Para la lectura del puerto 80h se pueden emplear tarjetas PCI comerciales que permiten visualizar el último código escrito.

6. Actualización de la ROM BIOS

La ROM BIOS de una placa base (o de una tarjeta de expansión) puede actualizarse fácilmente pues está almacenada en una memoria flash. La actualización de la ROM BIOS debe llevarse a cabo cuando se desea soporte para un dispositivo nuevo, incorporar un nuevo estándar o corregir errores de la ROM BIOS.

Para poder actualizar la ROM BIOS es fundamental identificar el fabricante de la placa base y acceder a su página web. Algunas ROM BIOS permiten identificar el fabricante a partir de un código que generan durante el arranque. En la actualidad los fabricantes de placas base disponen de herramientas que permiten identificar la versión de la ROM BIOS instalada en sus placas base y actualizarlas.

Es importante guardar antes de la actualización los parámetros de configuración de la BIOS si se han realizado cambios.

7. Borrado de la memoria CMOS de configuración de la BIOS

Puede ser necesario el borrado de los valores cuando los parámetros de configuración impiden la ejecución del POST o cuando se ha olvidado la contraseña de la BIOS.

La forma más simple de llevar a cabo este borrado es el empleo de utilidades específicas que se ejecutan sobre el sistema operativo. Otra posibilidad es modificando la posición de un *jumper* de la placa base que lleva a cabo el borrado de la memoria CMOS. Sin embargo, en este caso debe tenerse en cuenta que se borra todo el contenido de la memoria CMOS.

8. Parámetros de configuración de la BIOS

Los parámetros de configuración del sistema se almacenan en una memoria no volátil (usualmente denominada CMOS). Se puede acceder a los mismos para su visualización y modificación utilizando el programa de configuración de la BIOS. Los parámetros dependen del fabricante y la placa base, aunque los más importantes son comunes.

Los fabricantes suelen incluir valores por defecto que aseguran la estabilidad del sistema.

Cuando el conjunto de parámetros seleccionados impide el arranque puede ser necesario borrar la CMOS empleando un *jumper* de la placa base. El borrado de la CMOS produce la carga automática de los parámetros por defecto.

Los valores de algunos parámetros de la BIOS tienen influencia sólo durante el arranque. EL sistema operativo puede ignorarlos.

8.1 Seguridad

Es posible especificar contraseñas que controlan el arranque del sistema y la modificación de los parámetros de la BIOS. El olvido puede de estas contraseñas puede requerir el borrado de la memoria CMOS.

Es posible activar la protección de los sectores de arranque de discos duros para que no permita escribirlos. Sólo funciona cuando se accede al disco usando servicios de la BIOS.

Otro parámetro de seguridad es la protección de la BIOS frente a escrituras. Habitualmente esta protección también puede forzarse usando un *jumper* de la placa base.

8.2 Fecha y hora

Se puede visualizar y modificar la fecha y hora del sistema, las cuales son actualizadas por el RTC incluso con el PC apagado.

8.3 Arranque

Se puede seleccionar la secuencia de búsqueda de un sector de arranque (MBR) válido entre los dispositivos de almacenamiento del sistema.

También se puede seleccionar la posibilidad de hacer un arranque rápido, haciendo que el POST sea menos exhaustivo.

Algunas BIOS se pueden configurar mostrar o no un logotipo en lugar de mensajes del POST.

Otra opción permite escoger qué hacer cuando el equipo se apaga debido a un corte de luz: volver a encenderlo automáticamente o dejarlo apagado.

8.4 Monitorización del hardware

Se puede visualizar (no modificar) en tiempo real temperaturas (de la CPU, de la placa base, de la caja), velocidades de rotación de ventiladores (de la CPU, de la caja, de la fuente de alimentación) y tensiones de alimentación del sistema (+3,3 V, +5 V, +12V y la tensión del núcleo de la CPU).

8.5 Memoria

Activación y desactivación de niveles de caché. Poca utilidad (sistemas de tiempo real, comprobar si la caché está mal).

Activación y desactivación de la ECC de la caché. Su activación mejora la estabilidad a costa de una reducción de rendimiento muy pequeña.

Es posible visualizar la cantidad de memoria RAM instalada.

Pueden especificarse los parámetros temporales de los módulos de memoria (relativos a las señales RAS y CAS así como a la frecuencia de refresco). Lo mejor habitualmente es emplear la opción automática que los extrae del chip SPD.

El acceso a la ROM BIOS de la placa base y tarjetas de expansión es mucho más lento que el acceso a la memoria principal. La técnica de *shadowing* consiste en copiar su contenido a la memoria principal. En la práctica, el *shadowing* mejora muy poco el rendimiento, pues los *drivers* de los sistemas operativos modernos usan muy poco los servicios BIOS. En algunos casos el *shadowing* puede ocasionar problemas de estabilidad.

Un parámetro de configuración es la activación del *shadowing* por rangos de direcciones. Se puede configurar también la posibilidad de cachear las copias en RAM de ROM BIOS. Mejora muy poco el rendimiento y puede ocasionar problemas.

8.6 Dispositivos IDE (ATA/SATA)

Las BIOS actuales detectan automáticamente los cuatro dispositivos ATA posibles (maestro primario, esclavo primario, maestro secundario y esclavo secundario) y los dispositivos SATA.

La detección automática selecciona además los mejores parámetros posibles desde el punto de vista del rendimiento. Aunque suele existir una opción para

hacer una configuración manual de dispositivos de almacenamiento, en la actualidad no es conveniente utilizarla.

Se puede especificar el máximo tiempo que se espera en la detección de dispositivos ATA. Puede ser útil con discos antiguos que no son autodetectados en un arranque en frío.

Es interesante activar la característica SMART de los discos duros ATA/SATA que permite detectar prematuramente problemas en el disco.

En las BIOS que permiten RAID (habitualmente con discos SATA) existe una opción para escoger el modo de RAID.

8.7 Frecuencias y tensiones de alimentación

Una forma de incrementar el rendimiento a costa de la estabilidad e integridad del sistema es incrementar las frecuencias de trabajo de los dispositivos por encima de las especificaciones de los fabricantes. A esta técnica se la conoce como *overclocking*.

Para aumentar las frecuencias sin que se resienta demasiado la estabilidad es necesario aumentar las tensiones de alimentación. Un pequeño incremento de la frecuencia y de la tensión de alimentación trae consigo un gran incremento de la energía disipada y por lo tanto de la potencia demandada a la fuente.

El *overclocking* es un juego peligroso que no debería jugarse con equipos críticos.

Para practicar *overclocking* pueden tocarse la frecuencia del FSB u otros buses, el multiplicador de la CPU (si no está bloqueado, *locked*), la frecuencia del controlador de memoria. Incrementos en las frecuencias anteriores suelen requerir incrementos de la tensión de alimentación. Debe tenerse en cuenta que algunas de estas frecuencias pueden no ser independientes.

Otra forma de aumentar el rendimiento que no es estrictamente *overclocking* consiste en reducir los parámetros que especifican latencias de acceso a los módulos de memoria y sus frecuencias de refresco.

8.8 Controladores integrados

Las placas base incorporan controladores y puertos que admiten configuración en la BIOS, como, por ejemplo, controladores de sonido, USB, puertos serie, paralelo, etc. Además, en ocasiones puede ser necesario deshabilitar controladores que interfieren con otros (por ejemplo, una tarjeta de sonido integrada en la placa que interfiere con una conectada a una ranura PCI).

8.9 Gestión de energía

En los PCs actuales se lleva a cabo empleando la especificación ACPI (*Advanced Configuration and Power Interface*). Anteriormente se hacía con APM (*Advance Power Management*).

ACPI permite al sistema operativo configurar todos los dispositivos, incluyendo su gestión de energía. La implementación de ACPI reside en parte en la BIOS y

en parte en el sistema operativo, pero el control está en el sistema operativo, al contrario de lo que ocurría con APM.

ACPI define varios estados globales de consumo, denominados «estados globales», en los que puede estar un ordenador:

- G0 (S0): Trabajando. Estado normal cuando el ordenador está ejecutando instrucciones.
- G1: Durmiendo. El sistema está en alguno de los siguientes subestados[1]:
  - S1 (*Power on Suspend* o *Power on Standby*, POS, suspendido encendido): Procesador alimentado pero parado sin ejecutar instrucciones y con las cachés vaciadas.
  - S2: Estado de menor consumo que S1 pero no implementado habitualmente.
  - S3 (*Suspend to RAM*, STR, o suspendido en RAM). El estado del sistema se guarda en RAM y se deja de alimentar todo excepto la RAM. En Windows XP y algunas versiones de Linux se denomina *Suspender*, mientras que en Windows Vista se denomina *Dormir*.
  - S4 (*Suspend to Disk*, STD, o suspendido en disco). Casi todo apagado y el estado se guarda en disco. En Windows se denomina *Hibernar*. Un ordenador en este estado puede pasar a G3 (apagado mecánicamente) y todavía ser capaz de volver a recuperar el estado antes de dormirse.
- G2 o S5 (*Soft Off*, o apagado blando). Casi todo apagado y sin guardar estado. El sistema está casi apagado, pero puede responder a eventos que lo despierten. Cuando despierta debe reiniciarse. Éste es el estado habitual cuando se apaga el PC.
- G3 (*Mechanicall Off*, apagado mecánicamente). Todo apagado, excepto lo que se alimenta de la pila de la placa base.

Además, el estándar define varios estados para los dispositivos:

- D0: Totalmente encendido.
- D1 y D2: Estados de consumo reducido. Su significado depende del dispositivo.
- D3: Totalmente apagado.

Para la CPU, se definen una serie de estados específicos:

- C0: Es el estado de operación habitual.
- C1 (*Halt*, parado): El procesador no está ejecutando instrucciones, pero puede empezar a ejecutarlas casi inmediatamente.

[1] Entre paréntesis se dan los nombres con los que se suele encontrar en la BIOS, aunque el estándar ACPI no define estos nombres.

- C2 (*Stop-Clock*, reloj parado): El procesador mantiene estado visible desde el software pero puede llevarle un tiempo volver a despertar.
- C3 (*Sleep*, dormido): El procesador mantiene todo el estado pero no la caché.

Además también se definen estados P1 a P*n* con rendimiento y consumo diferentes en los que un componente puede encontrarse plenamente operativo. El significado de estos estados es dependiente del dispositivo, pero siempre el rendimiento del dispositivo en Pi es menor que en Pj si i < j.

Los parámetros de configuración ACPI más importantes de la BIOS son la definición de dispositivos que pueden despertar al PC (desde uno de los estados S1 a S5). Por ejemplo, pueden despertar al PC una alarma en el reloj de tiempo real, una tarjeta de red (WOL), un modem, un evento de teclado, etc.

Para que un dispositivo sea capaz de despertar al PC desde los estados S3, S4 o S5 es necesario que la fuente de alimentación sea capaz de proporcionar al menos 1 amperio para la tensión +5VSB.

En la actualidad muchos sistemas operativos proporcionan un modo de ahorro de energía que mezcla las ideas de suspensión a disco y a RAM: cuando el ordenador se suspende en este modo híbrido, el estado se mantiene tanto en disco como en RAM. De esta manera, el encendido es muy rápido (desde RAM) pero si alguna contingencia produce que se pierda el contenido de la RAM, no se pierde ningún dato porque se recupera desde disco.