Tema 1

Windows NT

Windows NT es un Sistema Operativo en Red que emplea una estructura cliente/servidor. Frente a las soluciones cliente/servidor tenemos las redes de igual a igual (peer to peer). Con NT tendremos uno o varios servidores que proporcionan recursos y clientes que usan esos recursos. Como clientes se pueden emplear equipos con muchos S.O. diferentes: DOS, Windows 3.1, Windows 95, Windows NT Workstation, UNIX, Macintosh OS y OS/2.

Características generales

Fiabilidad

- **Protección Memoria**: NT proporciona la seguridad de que cuando se ejecuten las aplicaciones del usuario no lo hagan en la zona de memoria que tiene asignada el kernel del sistema. Si una aplicación modificará la zona de memoria ocupada por NT podría dejar colgado el sistema. Por ello NT divide la memoria en anillos. El núcleo del sistema se ejecuta en el anillo 0, mientras que las aplicaciones del usuario se ejecutan en el anillo 3, es decir, las zonas de memoria donde se ejecutan ambos procesos son independientes.
- **Modelo de memoria plana**: NT es un S.O. de 32 bits real. Proporciona un modelo de memoria plana con 32 bits de direcciones, esto permite al S.O. direccionar hasta 4 Gb de memoria.
- **Modelo multitarea preferente**: NT usa la multitarea preferente para garantizar que todas las aplicaciones que se están ejecutando puedan acceder a los recursos del procesador. Es decir, evita que una aplicación monopolice el uso del procesador.
- **Sistema de ficheros transaccional**: NTFS es un sistema de ficheros avanzado y robusto que proporciona una mayor fiabilidad. Es capaz de recuperar una escritura errónea o incompleta. Es similar al TTS de NetWare.

Rendimiento

- **Más rápido**: Al ser un S.O. de 32 bits es mucho más rápido que los S.O. de 16 bits.
- **Multitarea y multiproceso**: Permite ejecutar varias tareas simultáneamente (multitarea) y además soporta varios procesadores en el mismo sistema (multiproceso). La versión Workstation sólo permite dos procesadores mientras el diseño la versión Server permite 32 aunque realmente su implementación sólo admite cuatro procesadores.
- **Multihilo**: Multithreading en inglés (thread hilo). Permite ejecutar distintas partes de una aplicación en paralelo. Cada aplicación consta de un hilo y ese hilo puede tener hilos hijo que se podrían ejecutar en paralelo (sobre todo cuanto contamos con más de un procesador, multiproceso). Cuando se dispone de varios procesadores es un crimen no emplear hilos para ejecutar todas aquellas partes de la aplicación que puedan ser ejecutadas en paralelo.
- **Procesadores RISC**: NT es independiente del hardware, no sólo soporta procesadores INTEL sino que soporta procesadores RISC como son: Power PC, Dec Alpha RISC y MIPSRISC.

Portabilidad

NT, como decíamos, no sólo funciona en plataformas INTEL sino que se puede ejecutar en otros sistemas.

- **Independencia del hardware**: NT tiene un diseño modular que le proporciona independencia del hardware. El único código específico que maneja el hardware reside en el **HAL** (Hardware Abstraction Layer). El HAL opera a bajo nivel traduciendo las operaciones de bajo nivel del S.O. a operaciones que puedan ser entendidas por el hardware específico que se está utilizando. Para dar soporte a un nuevo hardware, se escribe una nuevo HAL para que interactúe con ese hardware y se recompila el S.O..
- **Sistema de archivos configurables**: NT Server soporta múltiples sistemas de archivos: FAT y NTFS. Las versiones anteriores también podían emplear HPFS (High Performance File System) que es el sistema de archivos de OS/2. A partir de la versión 4 no se reconocen las particiones HPFS. Las particiones HPFS tienen que ser convertidas a FAT o NTFS antes de instalar NT.

Compatibilidad

Un elemento clave para analizar un S.O. es su capacidad para ejecutar las aplicaciones ya existentes. NT se ha diseñado para que sea capaz de ejecutar diferentes aplicaciones e interactúe con diferentes S.O.

- **Diseño de aplicaciones como subsistemas**: NT soporta aplicaciones DOS, Windows 3.x (16 bits), OS/2... NT, como decíamos, tiene un diseño modular lo que le permite ejecutar distintos tipos de aplicaciones. Para ello emplea distintos subsistemas. Para ejecutar un nuevo tipo de aplicación es necesario crear un nuevo subsistema.
- **Subsistema Windows-On-Windows (WOW)**: WOW proporciona compatibilidad con las aplicaciones Windows de 16 bits. Ofrece la posibilidad de ejecutar las aplicaciones Windows 3.x en un espacio de memoria compartida o separado.
- **Interfaz de Windows 95**: NT emplea un replica exacta de la interfaz de Windows 95 con algunos objetos menos y otros nuevos.
- **Interoperatividad con NetWare**: NT incluye el protocolo IPX/SPX para clientes NetWare 3.x y NetWare 4.x. Ofrece la capacidad de compartir archivos NetWare, importar cuentas de usuario y login scripts de un servidor NetWare. Se puede migrar de un servidor NetWare a un servidor NT.
- **Interoperatividad con UNIX**: NT se comunica con UNIX a través del protocolo TCP/IP. Incluye aplicaciones de conectividad básicas como FTP, Telnet o Ping.
- **Interoperatividad con Macintosh**: NT soporta el protocolo AppleTalk, que es el protocolo empleado en redes Macintosh. Por ejemplo, NT permite a los sistemas Macintosh la utilización de impresoras conectadas a una red NT.

Seguridad

La seguridad es uno de los aspectos más importante de un S.O. multiusuario.

- **Modelo de seguridad de dominio**: Se trata de un sofisticado sistema de acceso a la red. Dentro de la red existirán unos servidores especiales llamados controladores de dominio que serán los encargados de realizar todo el trabajo de autentificación de usuarios. La información de seguridad se guarda en una base de datos llamada SAM (Security Account Manager).
- **Sistema de archivos NTFS**: Este sistema de archivos complementa la seguridad del sistema, permitiendo a los administradores asignar distintos derechos de acceso a los ficheros y directorios. Además incluye un sistema de control de transacciones similar al TTS de NetWare y la utilidad Hot-Fix.
- **Características de tolerancia a fallos**: NT incluye características de tolerancia a fallos. Tolerancia a fallos significa la capacidad de un sistema para soportar los diferentes errores que se pueda producir durante su funcionamiento. La primera característica importante es el soporte RAID (Redundant Array of Inexpensive Disk) que es similar al disk mirroring y disk duplexing. Otra de las características que incluye es la inclusión de unidades de alimentación ininterrumpidas.
- **Entrada al sistema Ctrl+Alt+Del**: Esta secuencia produce en muchos equipos el reboot del sistema y su consecuente parada y pérdida de datos. Para evitar esto NT ha empleado esta secuencia para entrar al sistema.

Arquitectura del sistema

Comprender cómo funciona Windows NT y cual es su arquitectura es importante para programar aplicaciones para este entorno y recomendable para administrarlo. Vamos a hacer un recorrido por las profundidades de este sistema operativo.

Introducción

Windows NT presenta una arquitectura del tipo cliente-servidor. Los programas de aplicación son contemplados por el sistema operativo como si fueran clientes a los que hay que servir, y para lo cual viene equipado con distintas entidades servidoras.

Uno de los objetivos fundamentales de diseño fue el tener un núcleo tan pequeño como fuera posible, en el que estuvieran integrados módulos que dieran respuesta a aquellas llamadas al sistema que necesariamente se tuvieran que ejecutar en modo privilegiado (también llamado modo kernel, modo núcleo y modo supervisor). El resto de las llamadas se expulsarían del núcleo hacia otras entidades que se ejecutarían en modo no privilegiado (modo usuario), y de esta manera el núcleo resultaría una base compacta, robusta y estable. Por eso se dice que Windows NT es un sistema operativo basado en micro-kernel.

Por tanto en un primer acercamiento a la arquitectura distinguimos un núcleo que se ejecuta en modo privilegiado, y se denomina **Executive**, y unos módulos que se ejecutan en modo no privilegiado, llamados **subsistemas protegidos**.

Los programas de usuario (también llamados programas de aplicación) interaccionan con cualquier sistema operativo (SO en adelante) a través de un juego de llamadas al sistema propio de dicho sistema. En el mundo Windows en general, las llamadas al sistema se denominan API (Application Programming Interfaces, interfaces para la programación de aplicaciones). En Windows NT y en Windows 95 se usa una versión del API llamada API Win32.

Los subsistemas protegidos

Son una serie de procesos servidores que se ejecutan en modo no privilegiado, al igual que los procesos de usuario, pero que tienen algunas características propias que los hacen distintos.

Se inician al arrancar el s.o. y existen dos tipos: integrales y de entorno.

Un subsistema integral es aquel servidor que ejecuta una función crítica del s.o. (como por ejemplo el que gestiona la seguridad). Un subsistema de entorno da soporte a aplicaciones procedentes de s.o. distintos, adaptándolas para su ejecución bajo Windows NT.

Existen tres de este tipo:

- Win32, que es el principal, y proporciona la interfaz para aplicaciones específicamente construidas para Windows NT.
- POSIX, que soporta aplicaciones UNIX.
- OS/2, que da el entorno a aplicaciones procedentes del s.o. del mismo nombre.

El subsistema Win32

Es el más importante, ya que atiende no sólo a las aplicaciones nativas de Windows NT, sino que para aquellos programas no Win32, reconoce su tipo y los lanza hacia el subsistema correspondiente. En el caso de que la aplicación sea MS-DOS o Windows de 16 bits (Windows 3.11 e inferiores), lo que hace es crear un nuevo subsistema protegido. Así, la aplicación DOS o Win16 se ejecutaría en el contexto de un proceso llamado VDM (Virtual DOS Machine, máquina virtual DOS), que no es más que un simulador de un ordenador funcionando bajo MS-DOS. Las llamadas al API Win16 serían correspondidas con las homónimas en API Win32. Microsoft llama a esto WOW (Windows On Win32). El subsistema soporta una buena parte del API Win32. Así, se encarga de todo lo relacionado con la interfaz gráfica con el usuario (GUI), controlando las entradas del usuario y salidas de la aplicación. Por ejemplo, un buen número de funciones de las bibliotecas USER32 y GDI32 son atendidas por Win32,

ayudándose del Executive cuando es necesario. El funcionamiento como servidor de Win32 lo veremos un poco más adelante, en el apartado de llamadas a procedimientos locales.

El subsistema POSIX

La norma POSIX (Portable Operating System Interface for UNIX) fue elaborada por IEEE para conseguir la portabilidad de las aplicaciones entre distintos entornos UNIX. La norma se ha implementado no sólo en muchas versiones de UNIX, sino también en otros s.o. como Windows NT, VMS, etc. Se trata de un conjunto de 23 normas, identificadas como IEEE 1003.0 a IEEE 1003.22, o también POSIX.0 a POSIX.22, de las cuales el subsistema POSIX soporta la POSIX.1, que define un conjunto de llamadas al sistema en lenguaje C. El subsistema sirve las llamadas interaccionando con el Executive. Se encarga también de definir aspectos específicos del s.o. UNIX, como pueden ser las relaciones jerárquicas entre procesos padres e hijos (las cuales no existen en el subsistema Win32, por ejemplo, y que por consiguiente no aparecen implementadas directamente en el Executive).

El subsistema OS/2

Igual que el subsistema POSIX proporciona un entorno para aplicaciones UNIX, este subsistema da soporte a las aplicaciones del s.o. OS/2. Proporciona la interfaz gráfica y las llamadas al sistema; las llamadas son servidas con ayuda del Executive.

El subsistema proceso de inicio

El proceso de inicio (Logon Process) recibe las peticiones de conexión por parte de los usuarios. En realidad son dos procesos, cada uno encargándose de un tipo distinto de conexión: el **proceso de inicio local**, que gestiona la conexión de usuarios locales directamente a una máquina Windows NT; y el **proceso de inicio remoto**, el cual gestiona la conexión de usuarios remotos a procesos servidores de NT.

El subsistema de seguridad

Este subsistema interacciona con el proceso de inicio y el llamado **monitor de referencias de seguridad** (del que trataremos en el Executive), de esta forma se construye el modelo de seguridad en Windows NT. El subsistema de seguridad interacciona con el proceso de inicio, atendiendo las peticiones de acceso al sistema. Consta de dos subcomponentes: la **autoridad de seguridad local** y el **administrador de cuentas.**

El primero es el corazón del subsistema de seguridad, en general gestiona la política de seguridad local, así, se encarga de generar los permisos de acceso, de comprobar que el usuario que solicita conexión tiene acceso al sistema, de verificar todos los accesos sobre los objetos (para lo cual se ayuda del monitor de referencias a seguridad) y de controlar la política de auditorías, llevando la cuenta de los mensajes de auditoría generados por el monitor de referencias.

El **administrador de cuentas** mantiene una base de datos con las cuentas de todos los usuarios (login, claves, identificaciones, etc.). Proporciona los servicios de validación de usuarios requeridos por el subcomponente anterior.

El Executive

No debemos confundir el Executive con el núcleo de Windows NT, aunque muchas veces se usan (incorrectamente) como sinónimos. El Executive consta de una serie de componentes software, que se ejecutan en modo privilegiado, uno de los cuales es el núcleo. Dichos componentes son totalmente independientes entre sí, y se comunican a través de interfaces bien definidas. Recordemos que en el diseño se procuró dejar el núcleo tan pequeño como fuera posible y, como veremos, la funcionalidad del núcleo es mínima.

El administrador de objetos (Object Manager)

Se encarga de crear, destruir y gestionar todos los objetos del Executive. Tenemos infinidad de objetos: procesos, subprocesos, ficheros, segmentos de memoria compartida, semáforos, mutex, sucesos, etc. Los subsistemas de entorno (Win32, OS/2 y POSIX) también tienen sus

propios objetos. Por ejemplo, un objeto ventana es creado (con ayuda del administrador de objetos) y gestionado por el subsistema Win32. La razón de no incluir la gestión de ese objeto en el Executive es que una ventana sólo es innata de las aplicaciones Windows, y no de las aplicaciones UNIX o OS/2. Por tanto, el Executive no se encarga de administrar los objetos relacionados con el entorno de cada s.o. concreto, sino de los objetos comunes a los tres.

El administrador de procesos (Process Manager)

Se encarga (en colaboración con el administrador de objetos) de crear, destruir y gestionar los procesos y subprocesos. Una de sus funciones es la de repartir el tiempo de CPU entre los distintos subprocesos. Suministra sólo las relaciones más básicas entre procesos y subprocesos, dejando el resto de las interrelaciones entre ellos a cada subsistema protegido concreto. Por ejemplo, en el entorno POSIX existe una relación filial entre los procesos que no existe en Win32, de manera que se constituye una jerarquía de procesos. Como esto sólo es específico de ese subsistema, el administrador de objetos no se entromete en ese trabajo y lo deja en manos del subsistema.

El administrador de memoria virtual (Virtual Memory Manager)

Windows NT y UNIX implementan un direccionamiento lineal de 32 bits y memoria virtual paginada bajo demanda. El VMM se encarga de todo lo relacionado con la política de gestión de la memoria. Determina los conjuntos de trabajo de cada proceso, mantiene un conjunto de páginas libres, elige páginas víctima, sube y baja páginas entre la memoria RAM y el archivo de intercambio en disco, etc.

La facilidad de llamada a procedimiento local (LPC Facility)

Este módulo se encarga de recibir y enviar las llamadas a procedimiento local entre las aplicaciones cliente y los subsistemas servidores.

El administrador de entrada/salida (I/O Manager)

Consta de varios subcomponentes: el **administrador del sistema de ficheros**, el **servidor de red**, el **redirector de red**, los **controladores de dispositivo del sistema** y el **administrador de cachés.**

Buena parte de su trabajo es la gestión de la comunicación entre los distintos controladores de dispositivo, para lo cual implementa una interfaz bien definida que permite el tratamiento de todos los controladores de una manera homogénea, sin preocuparse del funcionamiento específico de cada uno. Trabaja en conjunción con otros componentes del Executive, sobre todo con el VMM. Le proporciona la E/S síncrona y asíncrona, la E/S a archivos asignados en memoria y las caches de los ficheros. El administrador de caches no se limita a gestionar unos cuantos buffers de tamaño fijo para cada fichero abierto, sino que es capaz de estudiar las estadísticas sobre la carga del sistema y variar dinámicamente esos tamaños de acuerdo con la carga. El VMM realiza algo parecido en su trabajo.

El monitor de referencias a seguridad

Este componente da soporte en modo privilegiado al subsistema de seguridad, con el que interacciona. Su misión es actuar de alguna manera como supervisor de accesos, ya que comprueba si un proceso determinado tiene permisos para acceder a un objeto determinado, y monitoriza sus acciones sobre dicho objeto. De esta manera es capaz de generar los mensajes de auditorías. Soporta las validaciones de acceso que realiza el subsistema de seguridad local.

El núcleo (Kernel)

Situado en el corazón de Windows NT, se trata de un micro-kernel que se encarga de las funciones más básicas de todo el sistema operativo: ejecución de subprocesos, sincronización multiprocesador, manejo de las interrupciones hardware.

El nivel de abstracción de hardware (HAL)

Es una capa de software incluida en el Executive que sirve de interfaz entre los distintos controladores de dispositivo y el resto del sistema operativo. Con el HAL, los dispositivos se presentan al s.o. como un conjunto homogéneo con el cual interacciona a través de un conjunto de funciones bien definidas. Estas funciones son llamadas tanto desde el s.o. como desde los propios controladores. Permite a los controladores de dispositivo adaptarse a distintas arquitecturas de E/S sin tener que ser modificados en gran medida. Además oculta los detalles hardware que conlleva el multiproceso simétrico de los niveles superiores del s.o.