Módulo 1: Introducción

Conceptos

User Mode and Kernel Mode

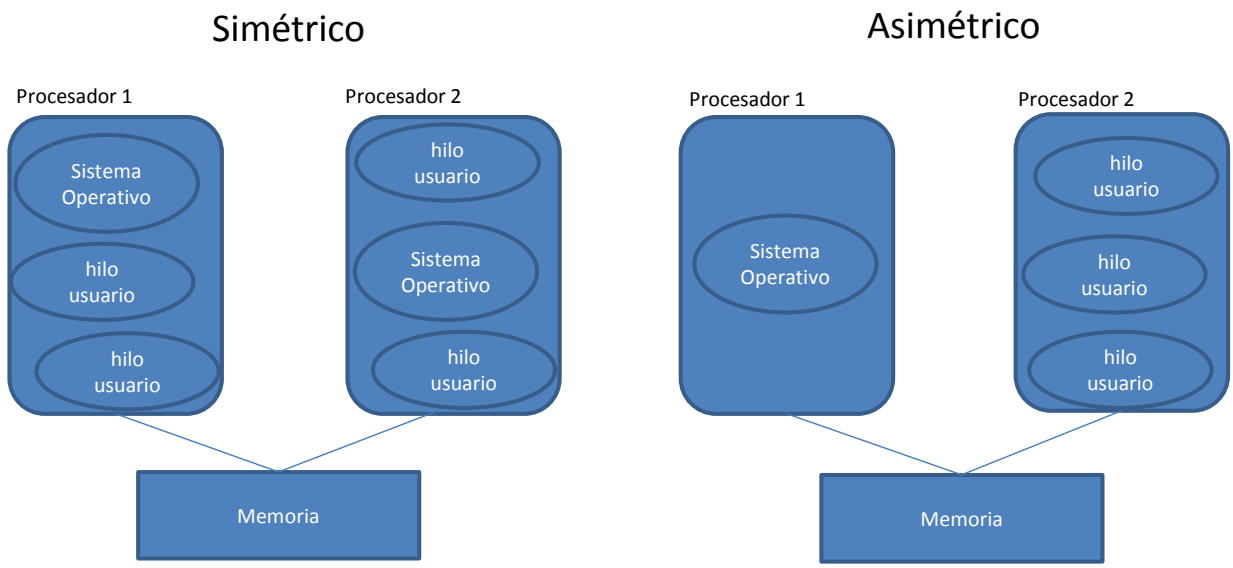
Windows usa dos modos/niveles de acceso del procesador. Aplicaciones de usuario corren en “User Mode”, código del sistema operativo corren en “Driver Mode”.

La arquitectura x86 y x64 define 4 niveles de privilegio o anillos (rings). Windows usa el nivel de privilegio 0 (anillo 0) para el Kernel Mode y privilegio 3 (anillo 3) para el User Mode.

Symmetric/Asymmetric multiprocessing

Cuando una computadora tiene más de 1 procesador, este puede ejecutar múltiples hilos simultáneamente.

Windows es un sistema operativo “Symmetric multiprocessing” (SMP), no existe un procesador central. A diferencia del “Asymmetric multiprocessing”, donde se selecciona un procesador dedicado para ejecutar el código del Kernel Mode y los demás procesadores ejecutan códigos del User Mode.



Windows soporta sistemas multicore nativamente, el código de Windows SMP trata los núcleos (cores) como si fueran procesadores individuales.

Máximo número de Procesadores en 32 bits 32

Máximo número de Procesadores en 64 bits 64

Windows Vista y Windows Server 2008 soportan:

Hyperthreading: Tecnología introducida por Intel que provee varios procesadores lógicos dentro de un procesador físico.

NUMA (non-uniform Memory architecture): Los procesadores son agrupados en pequeñas unidades llamadas nodos, cada nodo tiene su propio procesador y su propia memoria.

Windows Vista y Windows Server 2008 tienen un Kernel unificado a comparación de versiones anteriores, sin importar si son para sistemas uniprocesadores o multiprocesadores con excepción de las versiones de 32 bits de Windows.

Processes

Un conjunto de recursos usados para ejecutar una instancia de un programa.

Un proceso de Windows comprende de lo siguiente:

- Private virtual address space.
- Programa ejecutable.
- Lista de handles
- Access Token
- Process ID
- Al menos un hilo (Thread)

Cada proceso sabe cuál es su proceso creado (Parent Process).

Thread

Un hilo es la entidad dentro de un proceso, sin ella el programa de proceso no se puede ejecutar.

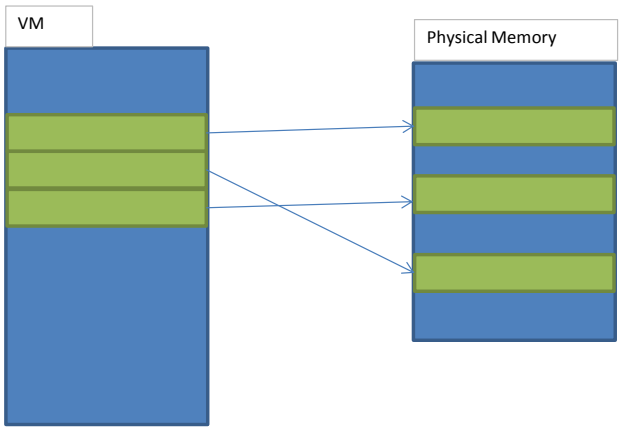
- Dos stacks (Kernel, User)
- Thread-local storage (TLS)
- Thread ID

Fibers permite a una aplicación programar la ejecución de sus propios hilos. Los Fibers son también llamados Lightweight Threads, están implementados en el modo usuario (Kernel32.dll).

Virtual Memory

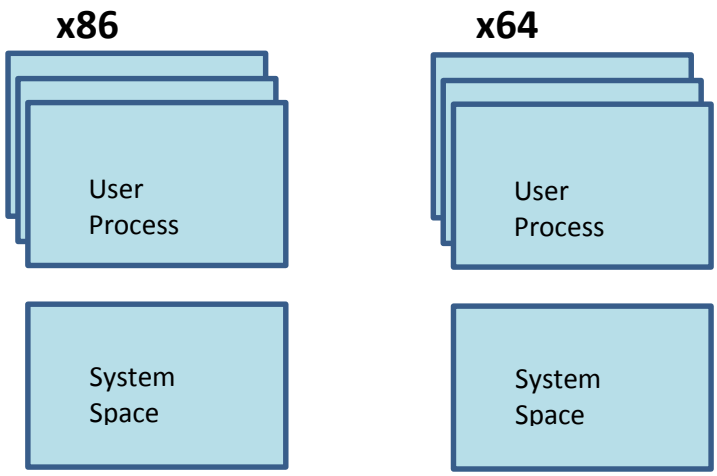
Memoria virtual provee a cada proceso la ilusión de tener su propia memoria privada (Private Address Space).

A momento de ejecución **Memory Manager** traduce la dirección virtual a dirección física.



x86 total de memoria virtual es de 4GB, 2GB Process Space, 2GB System Space.

x64 total de memoria virtual es de 16TB, 8TB Process Space, 8TB System Space.



Physical Address Extension

Característica de los procesadores x86 que permite a los sistemas de 32-bit utilizar 64 GB de memoria física.

Windows Client versions and Server Versions

Windows Vista: 6 versiones

Windows 2008: 5 versiones

Comparten los mismos archivos del sistema: Ntoskrnl.exe, HALL, Device drivers...

Diferencias:

- Numero de procesadores
- Capacidad de Memoria física
- Máximo número de conexiones permitidas
- Soporte de algunas características como: BitLocker.

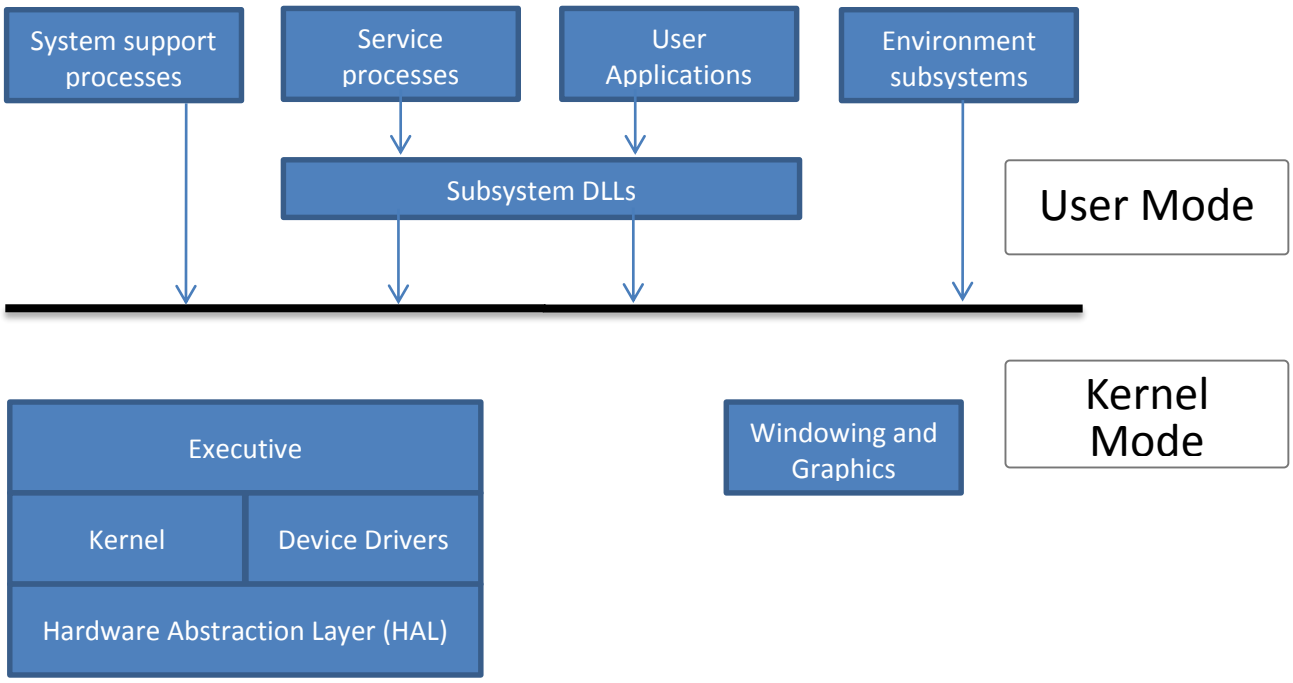
	#Procesadores (32 bits)	Memoria Física (32 bits)	#Procesadores (64 bits)	Memoria Física (Itanium)	Memoria Física (64 bits)
Vista: Started Edition	1	4 GB	No aplicable	No aplicable	No aplicable
Vista: Home Basic	1	4 GB	1	No aplicable	8 GB
Vista: Home Premium	1	4 GB	1	No aplicable	16 GB
Vista: Business	2	4 GB	2	No aplicable	128 GB
Vista: Enterprise	2	4 GB	2	No aplicable	128 GB
Vista: Ultimate	2	4 GB	2	No aplicable	128 GB
2008: Web server	2	4 GB	2	No aplicable	32 GB
2008: Standard	4	4 GB	4	No aplicable	32 GB
2008: Enterprise	8	32 GB	8	No aplicable	2048 GB
2008: Datacenter	32	64 GB	64	2048 GB	2048 GB
2008: Itanium-Based	No aplicable	No aplicable	64	2048 GB	No aplicable

Checked Build

Versión Debug llamada Checked Build útil para desarrolladores de drivers para detectar errores. El código adicional del checked build son Macros ASSERT y mensajes de tracing.

Componentes de Windows

Diagrama básico de los principales componentes de la arquitectura de Windows.



User Mode

System Support Processes.- Servicios no controlados por el "Service Control Manager".

Service Processes.- Windows services (servicios controlados por Service Control Manager).

User Applications.- Puede ser cualquiera de los 5 tipos (Windows 64bits, 32bits, 16bits, MS-DOS 16bits o POSIX 32bits).

Environment Subsystem.- Windows NT viene con 3 Environment subsystems (Windows, POSIX y OS/2).

OS/2 – Solo hasta Windows 2000

POSIX – Actualmente mejorado: Subsystem para Unix-based Applications (SUA).

Windows Subsystem controla el teclado, ratón y la visualización (siempre está presente).

Subsystem DLLs.- Traducir funciones documentadas (APIs) a funciones no documentadas (System Service Calls).

Kernel Mode

Executive.- Contiene los servicios básicos del sistema operativo como ser: Memory Manager, Object Manager, Cache Manager…

Kernel.- Provee estructuras básicas para ser usadas por el Executive, provee funciones del sistema operativo como ser: Thread scheduling, interrupt dispatching…

Device Drivers.- Módulos cargables del Kernel Mode. Interfaz entre el I/O Manager y el Hardware. No interactúa directamente con el hardware, hace llamadas a través del HAL.

Hardware Abstraction Layer (HAL).- Aísla el Kernel, Executive y Device driver de la diferencias del hardware. Windows Vista y 2008 tiene la habilidad de detectar que HAL usar al momento de arranque.