Modulo 1

Windows Internals: Introducción

César Cardona

Fundación Jala

Contenido

Conceptos

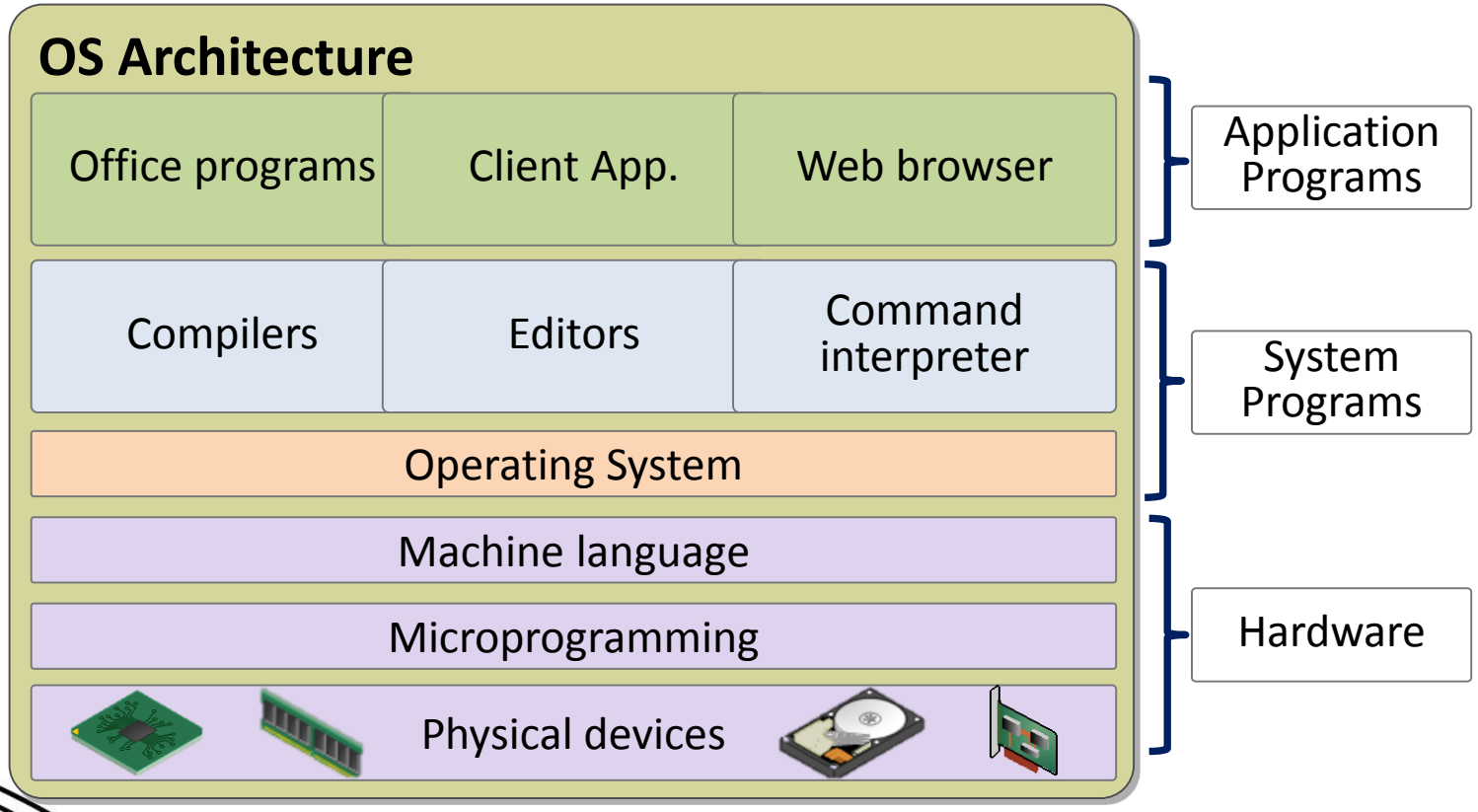
- Sistema Operativo
- User/Kernel Mode
- Symmetric/Asymmetric Multiprocessing
- Process, Threads
- Virtual Memory
- Physical Address Extension
- Windows client and server versions
- Checked Build

Componentes de Windows

- User Mode
- Kernel Mode

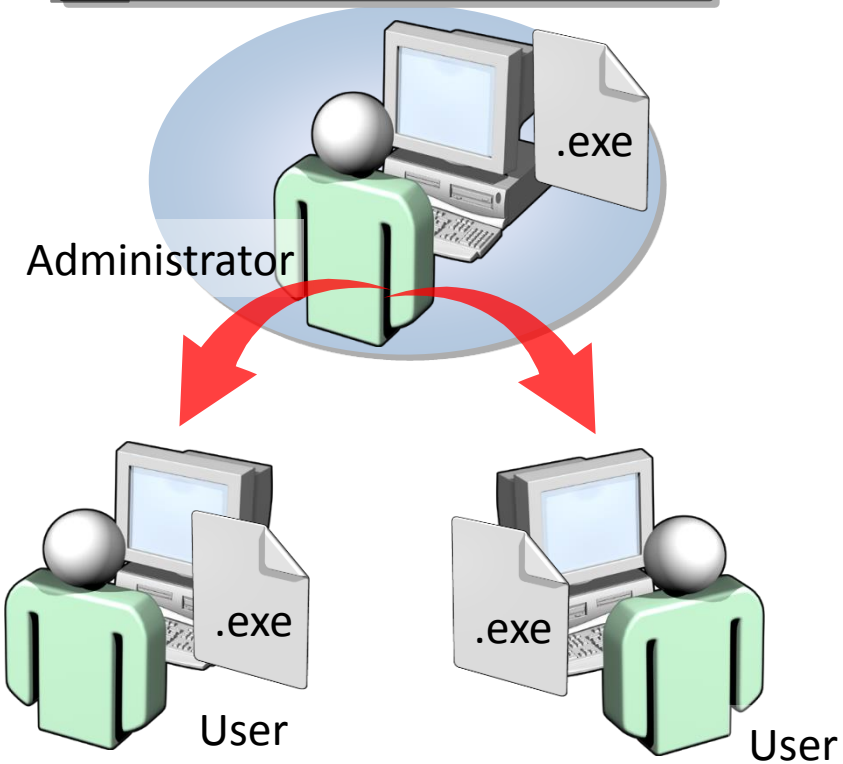
Conceptos de un Sistema Operativo

- Un Sistema Operativo es intermediario entre el usuario y el hardware de una computadora:
  - Facilidad de uso (para el usuario)
  - Eficiencia (para el hardware)



Instalando una aplicación

1. Correr la aplicación
2. Instalar la aplicación



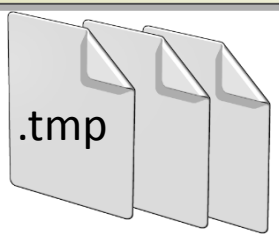
Configurar la aplicación

4. Escribir entradas en el registro

Registry Editor

- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

5. Crear archivos temporales

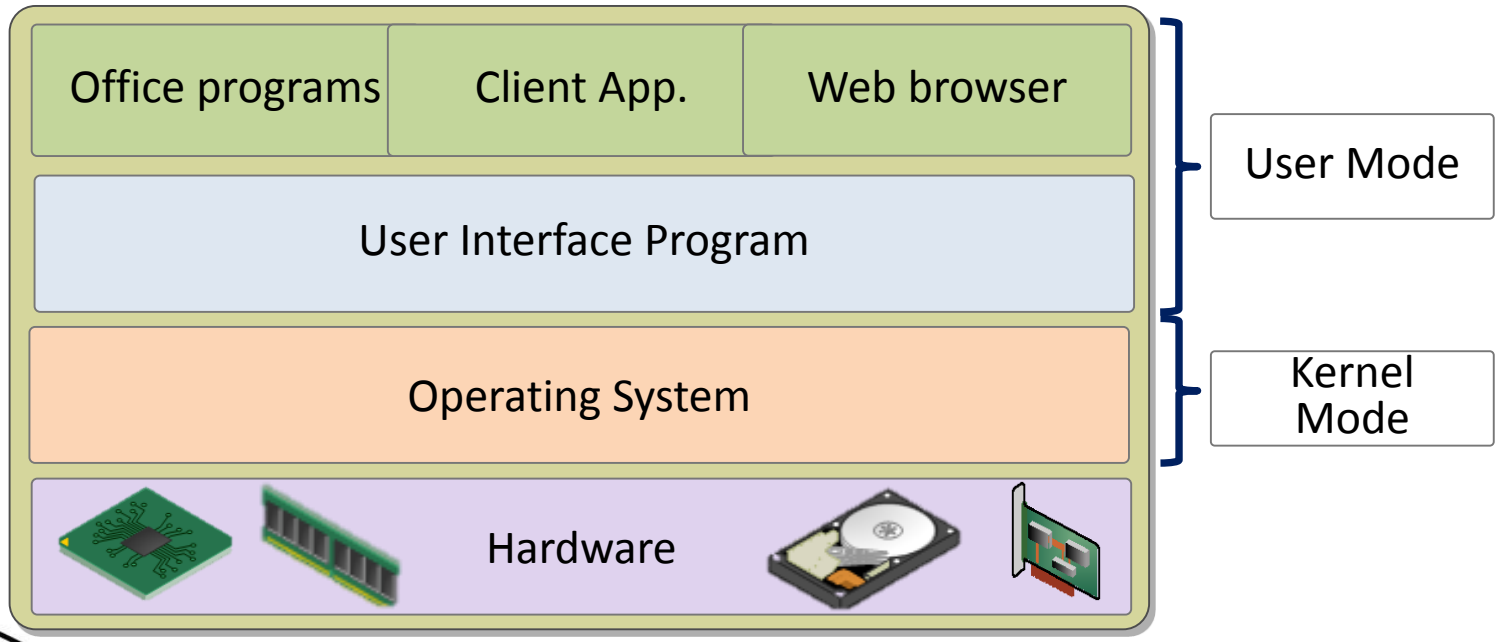


6. Escribir archivos en directorio de instalación de la aplicación

User Mode / 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.



User Mode / Kernel Mode

Kernel Mode:

- Modo privilegiado
- Asunciones estrictas acerca de la fiabilidad / seguridad de código.
- Reside en memoria:
  - Administración de CPU, memoria, dispositivos de entrada / salida.
  - Administración multiprocesador, diagnóstico, pruebas.
  - Partes del sistema de archivos y de la interfaz de red.

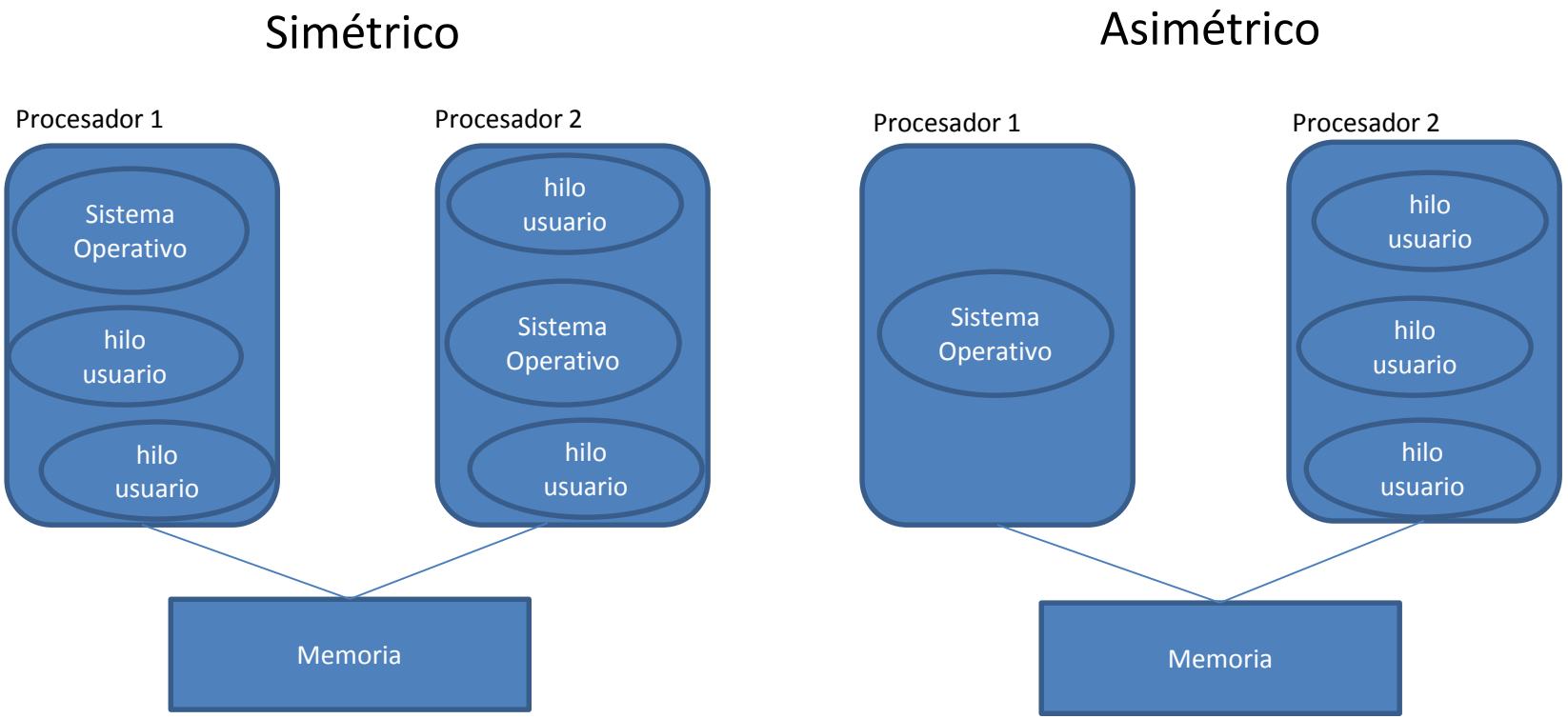
User Mode:

- Más flexible.
- Más sencillo de mantener y depurar.
  - Compilador, ensamblador, intérprete.
  - La gestión del sistema de archivos, gestión de redes.
  - Editores, hojas de cálculo, aplicaciones de usuario

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.

Symmetric/Asymmetric multiprocessing



Processes / Threads

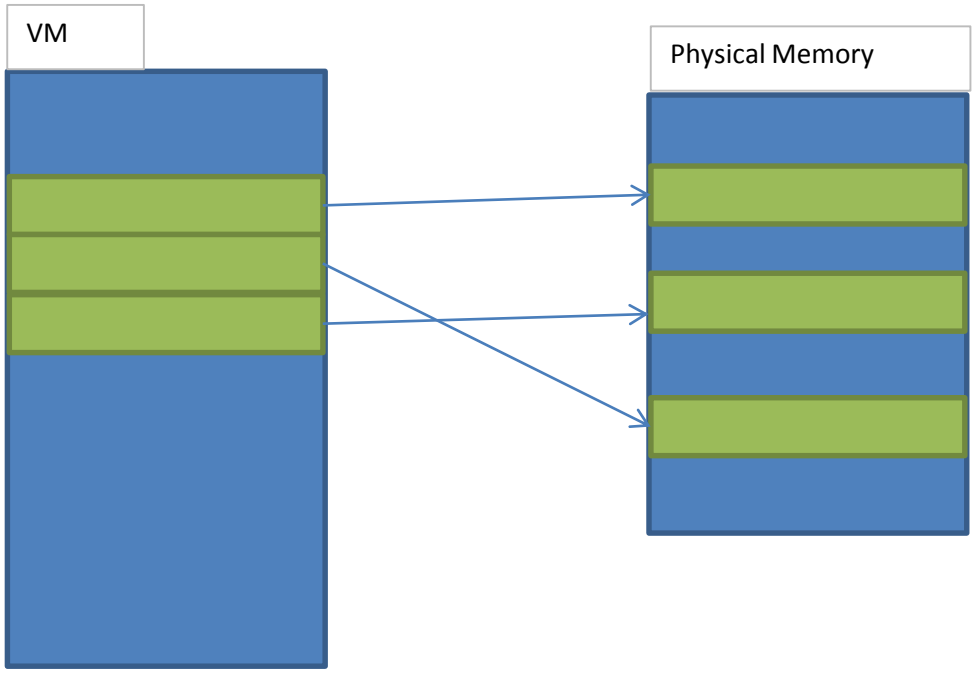
Processes
Un conjunto de recursos usados para ejecutar una instancia de un programa.

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

Virtual Memory

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

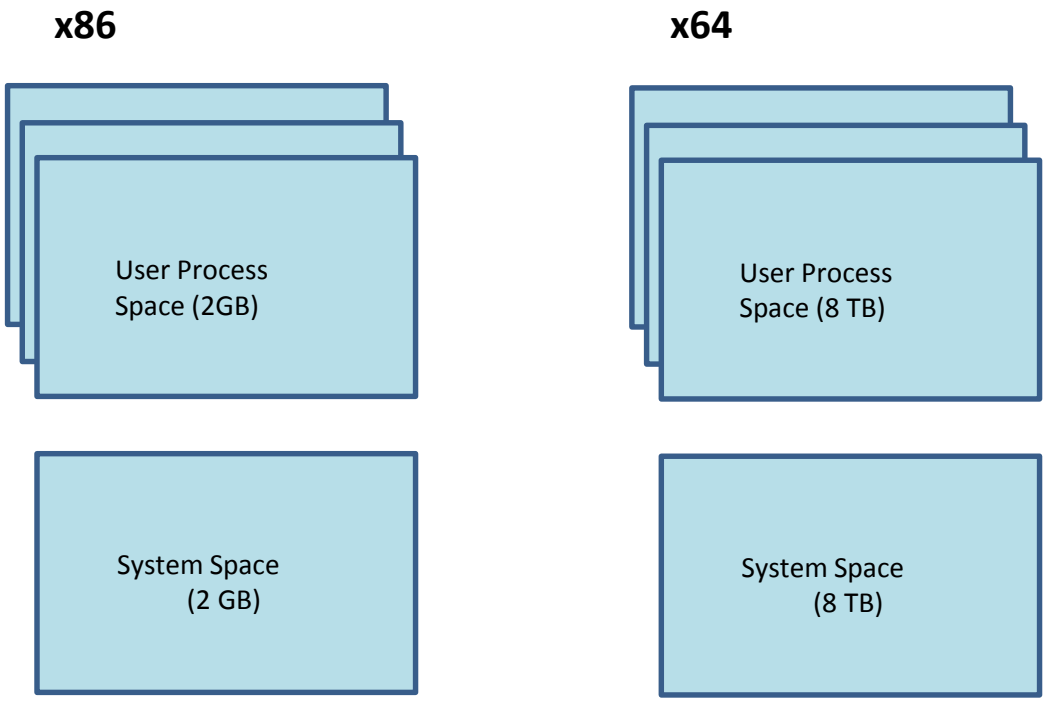
A momento de ejecución **Memory Manager** traduce la dirección virtual a dirección física.



Virtual Memory

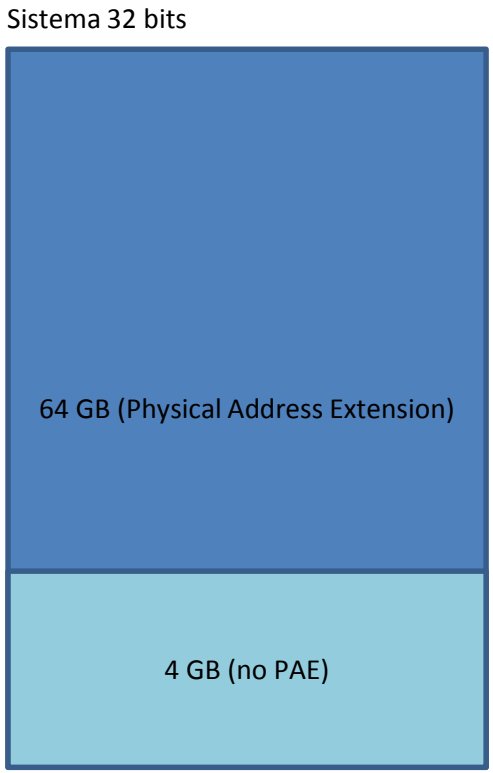
X86 total de memoria virtual es de 4GB, 2GB Process Space, 2GB System Space.

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.

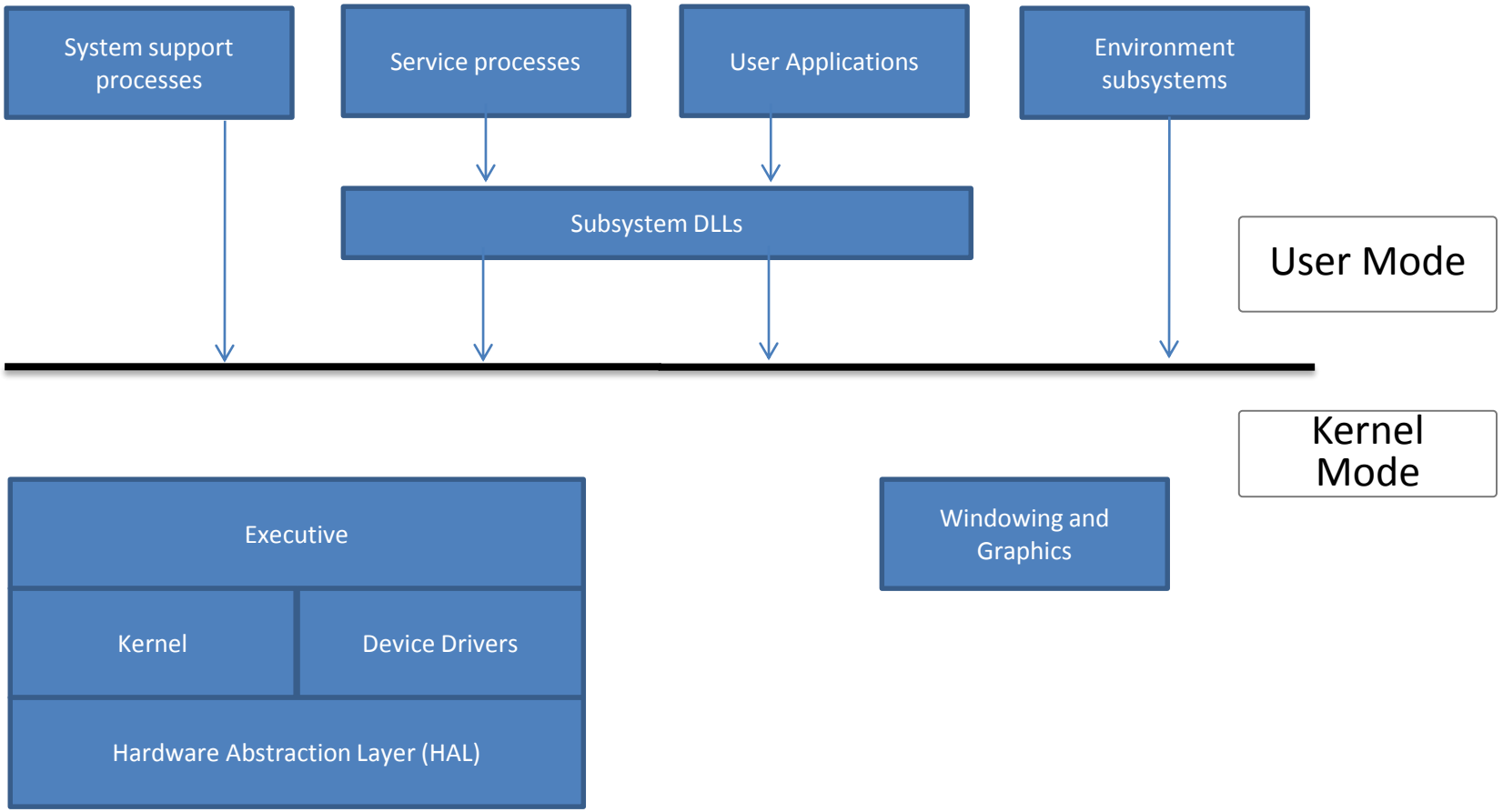


Windows Client versions and Server Versions

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

	#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

Componentes 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).
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.
The windowing and graphics system.- implementa la función de interfaz gráfica de usuario (GUI)

Kernel Mode

Nombre de Archivo	Componentes
Ntoskrnl.exe	Executive and kernel.
Ntkrnlpa.exe (32-bit systems only)	Executive and kernel, con soporte para Physical Address Extension (PAE)
Hal.dll	Hardware abstraction layer
Win32k.sys	Kernel-mode parte del Windows subsystem.
Ntdll.dll	Soporte interno para funciones y System Service para el de envío de datos a las funciones del Executive.
Kernel32.dll, Advapi32.dll, User32.dll, Gdi32.dll	Core Windows subsystem DLLs