* Versión de la tecnología Intel® Turbo Boost ‡1,0

La Tecnología Intel® Turbo Boost aumenta dinámicamente la frecuencia del procesador cuando sea necesario sacando provecho de la ampliación térmica y de energía para que tenga un impulso en la velocidad cuando lo necesite, y un aumento en la eficacia energética cuando no

* Idoneidad para la plataforma Intel® vPro™

es un conjunto de capacidades de seguridad y administración desarrolladas en el procesador diseñado para abordar cuatro áreas fundamentales de seguridad en TI:

1) Administración de amenazas, incluida la protección de rootkits, virus y malware

2) Identidad y protección de punto de acceso al sitio web

3) Protección de datos confidenciales personales y de negocio

4) Monitoreo remoto y local, corrección y reparación de PC y estaciones de trabajo.

* Tecnología Hyper-Threading Intel® ‡

La Tecnología Intel® Hyper-Threading ofrece dos cadenas de procesamiento por núcleo físico. Las aplicaciones con muchos subprocesos pueden realizar más trabajo en paralelo, completando antes las tareas.

Cada canal de datos (hilo, o *thread* en inglés) es programado y ejecutado de manera individual en el núcleo. **Con HyperThreading lo que se consigue es que cada núcleo asigne recursos a dos hilos a la vez.**

La tecnología Hyper-threading simula, de cara a los programas, que existen dos microprocesadores por núcleos del procesador.

* Tecnología de virtualización Intel® (VT-x) ‡

La tecnología de virtualización (VT-x) Intel® permite que una plataforma de hardware funcione como varias plataformas "virtuales". Ofrece mejor capacidad de administración limitando el tiempo de inactividad y manteniendo la productividad a través del aislamiento de las actividades de cómputo en particiones separadas.

* Intel® VT-x con tablas de páginas extendidas (EPT) ‡
* Intel® VT-x con Tablas de página extendidas (EPT), también conocidas como Traducción de direcciones de segundo nivel (SLAT), brinda aceleración a las aplicaciones virtualizadas con uso intensivo de memoria. Las Tablas de página extendidas en las plataformas de Tecnología de virtualización de Intel® reducen los costos adicionales de memoria y alimentación, y aumentan el rendimiento de la batería mediante la optimización del hardware de la administración de la tabla de página.
* Intel® 64 ‡Yes

La arquitectura Intel® 64 ofrece procesamiento informático de 64 bits en plataformas para servidores, estaciones de trabajo, PC y portátiles cuando se la combina con software compatible.¹ La arquitectura Intel 64 mejora el desempeño permitiendo que los sistemas direccionen más de 4 GB de memoria física y virtual.

* Conjunto de instrucciones 64-bit

Una serie de instrucciones hacen referencia al conjunto básico de comandos e instrucciones que un microprocesador comprende y puede llevar a cabo. El valor que se muestra representa con qué conjunto de instrucciones de Intel es compatible este procesador.

* Extensiones de conjunto de instrucciones Intel® SSE4.2

Las extensiones de conjunto de instrucciones son instrucciones adicionales que pueden aumentar el rendimiento cuando se realizan las mismas operaciones en múltiples objetos de datos. Estas pueden incluir a SSE (Streaming SIMD Extensions) y AVX (Advanced Vector Extensions).

* Estados de inactividad

Los estados de inactividad (estados C) se utilizan para ahorrar energía cuando el procesador esté inactivo. C0 es el estado operacional, lo que significa que la CPU está funcionando correctamente. C1 es el primer estado de inactividad, C2 el segundo, etc., donde se realizan más acciones de ahorro de energía para estados C con valores numéricos más altos.

* Tecnología Intel SpeedStep® mejorada

La tecnología Intel SpeedStep® mejorada es un medio avanzado para permitir un desempeño muy alto y a la vez satisfacer la necesidad de conservación de energía de los sistemas portátiles. La tecnología Intel SpeedStep® tradicional conmuta el voltaje y la frecuencia en tándem entre niveles altos y bajos en respuesta a la carga del procesador. La Tecnología Intel SpeedStep® mejorada se desarrolla en esa arquitectura utilizando las estrategias de diseño como separación entre cambios de voltaje y frecuencia, y partición de reloj y recuperación.

* Conmutación según demanda Intel®

La conmutación según demanda de Intel® es una tecnología de administración de la energía donde el voltaje aplicado y la velocidad del reloj de un microprocesador se mantienen en los niveles mínimos necesarios hasta que se necesite más energía de procesamiento. Esta tecnología fue presentada como tecnología Intel SpeedStep® en el mercado de servidores.

* Tecnologías de monitoreo térmico

Las tecnologías de monitor térmico protegen el paquete y el sistema del procesador de fallas térmicas a través de varias funciones de administración térmica. Un Sensor digital térmico (DTS) en matriz detecta la temperatura del núcleo, y las funciones de administración térmica reducen el consumo de energía del paquete y, por lo tanto, la temperatura cuando se requiere para mantener normales los límites de operación.

* Intel Rapid Storage Technology

Es una aplicación basada en Windows que proporciona un mejor rendimiento y fiabilidad para los sistemas equipados con discos SATA. Cuando se utiliza una o varias unidades de disco SATA, puede aprovechar las ventajas de un mejor rendimiento y un menor consumo de energía. Cuando se utiliza más de un disco, puede aumentar la protección contra la pérdida de datos, en caso de que falle el disco (RAID).

* Smart Caché

Algunas arquitecturas optan por compartir la memoria caché L2 entre diferentes núcleos para una mejor relación rendimiento/costo y una mejor asignación de recursos.

Uso eficiente de la caché L2

Si un núcleo está inactivo, el otro núcleo toma todo el caché compartido

Reduce la subutilización de recursos

Flexibilidad para programadores

Permite más oportunidades para compartir datos para subprocesos que se ejecutan en núcleos separados que comparten caché

Un núcleo puede pre/post procesar datos para el otro núcleo

Mecanismos alternativos de comunicación entre núcleos.

Reduce la complejidad de coherencia de caché

Se redujo el uso compartido falso debido a la memoria caché compartida

Menos carga de trabajo para mantener la coherencia, en comparación con la arquitectura de caché privada

Reduce la redundancia de almacenamiento de datos

Los mismos datos solo deben almacenarse una vez

Reduce el tráfico de buses en la parte delantera

El intercambio efectivo de datos entre núcleos permite que las solicitudes de datos se resuelvan en el nivel de caché compartida en lugar de ir a la memoria del sistema

* Memoria Intel Optane

La memoria Intel® Optane™ es un tipo de memoria no volátil que se encuentra entre la memoria del sistema y el almacenamiento.

Al combinarse con el controlador de la Tecnología de almacenamiento Intel® Rapid, administra varios niveles de almacenamiento y presenta una sola unidad virtual al sistema operativo, lo cual permite que los datos de uso frecuente residan en el nivel de almacenamiento más rápido.

* **QPI (Intel Quick Path Interconnect):**

El Intel Quick Path Interconnect ("QuickPath", "QPI") es una conexión punto a punto con el procesador desarrollado por Intel para competir con HyperTransport de AMD. Sustituye al FSB y es implementado en microprocesadores de gama alta.

Conecta los procesadores la memoria y el hub de entrada salida.

Cubre dos tipos de configuraciones:

* Equipos con varias tarjetas gráficas y en los cuales el controlador PCIe no está dentro del procesador.
* Equipos con varios procesadores en la misma placa base. Para esto, se hace necesario tener un gran ancho de banda de salida desde la CPU.

 Una versión más potente de esta interfaz es Intel® UPI (Ultra Path Interconnect)

* DMI (Direct Media Interface):

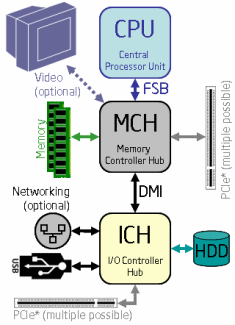
DMI tecnología de Bus que se utiliza en procesadores **Intel Core i3, i5 e i7**. La diferencia básica en la arquitectura es que el procesador se comunica a través de un canal diferente con la RAM, un canal diferente con PCIe y un canal DMI para comunicarse con todos los demás componentes del equipo. Esto aumenta el rendimiento de manera significativa.

## Diferencia entre el FSB y DMI

## ****FSB (Front Side Bus)****

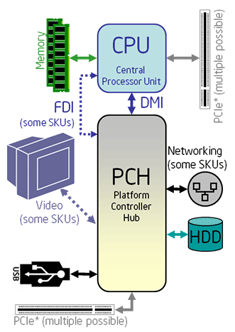
FSB es una tecnología de Bus que se utiliza en procesadores**Core 2 Quad / Duo** y anteriores. FSB permite que el procesador se comunique con otros componentes del ordenador, incluyendo la memoria, PCI, Video, así como dispositivos IO como USB, disco duro, red, etc.

Todo lo que entra y sale del procesador pasa a través de FSB.  Se puede ver en el **diagrama** que está a continuación, un típico procesador Core 2 Duo y los canales de comunicación del FSB.



## DMI (Direct Media Interface)

DMI tecnología de Bus que se utiliza en procesadores **Intel Core i3, i5 e i7**. La diferencia básica en la arquitectura es que el procesador se comunica a través de un canal diferente con la RAM, un canal diferente con PCIe y tercera DMI canal para comunicarse con todos los demás componentes del equipo. Esto aumenta el rendimiento de manera significativa. En el diagrama siguiente se puede ver una **arquitectura Core i7** típica



**Seguridad y fiabilidad**

* Nuevas instrucciones de AES Intel®
* Tecnología Intel® Trusted Execution
* Bit de desactivación de ejecución