|  |  |  |
| --- | --- | --- |
| **Fecha de entrega:** 20 de octubre de 2017 | **Título de la tarea:** Me  mory Management Unit. How it is used inside of compute. | **Número de la tarea:** 2.3 |
| **Grupo:** 3CM3 | **Alumno:** Estrada Granados Diego | **Unidad de aprendizaje:** Arquitectura de Computadoras |

**Memory Management Unit. How it is used inside of compute.**

La Unidad de Manejo de Memoria del procesador trabaja con el sistema de memoria caché para controlar los accesos a la memoria externa. La MMU también controla la traducción de direcciones virtuales a direcciones físicas.

La MMU controla la tabla del hardware que contiene los accesos a las tablas de dirección de la memoria principal. En cada solicitud tanto segura como no segura, un único conjunto de tablas de páginas de dos niveles almacenados en la memoria principal controla el contenido de las instrucciones y datos. La dirección virtual traducida se coloca en el TLB, asociado con un identificador de tabla no seguro que permite la existencia de entradas seguras y no seguras.

La arquitectura de la MMU permite el control preciso de un sistema de memoria. Esto se controla por un conjunto de asignaciones de direcciones virtuales y físicas y propiedades de memoria asociadas dentro de las estructuras TLB dentro de la MMU. El contenido de los TLB se gestiona mediante búsquedas de traducción de hardware desde un conjunto de tablas de traducciones de memoria. Para evitar que se requiera na invalidación de TLB en un cambio de contexto, podemos marcar cada asignación de dirección virtual a dirección física asociada a un espacio de aplicación particular o como global para todos los espacios de aplicación. Solo las asignaciones globales y las de espacio de aplicaciones actuales están habilitadas en cualquier momento.

El conjunto de propiedades asociadas con cada entrada de TLB contiene:

**Control de permiso para el acceso de memoria.**

Controla el acceso para lectura, escritura en el área de memoria. Cuando se intenta acceder a la memoria sin el permiso necesario se envía una señal de aborto de memora es enviada al procesador. El nivel de acceso a la memoria puede verse afectado por el modo de usuario que ejecute la aplicación (privilegiado o usuario) y también podría verse afectado por el uso de dominios.

**Atributos de la región de memoria.**

Describen propiedades de una región de memoria. Entre algunos ejemplos se encuentran *Strongly Ordered, Device, cacheable Write-Through*, y *cacheable Write-Back.* Si no se encuentra una entrada para una dirección virtual en una TLB, el hardware busca automáticamente un conjunto de tablas de dirección en la memoria para crear una entrada TLB. Este proceso es conocido como *translation table walk.* La arquitectura MMU también permite que las entradas de un TLB específico se bloqueen en un TLB. Esto asegura que los accesos a las áreas de memoria asociadas nunca requieran una búsqueda *translation table walk* minimizando el tiempo para acceder al código y las rutinas en tiempo real.

**Atributo de región de memoria no segura.**

Este atributo define cuando la memoria de destino es o no es segura.

**Secuencia de acceso de memoria.**

Cuando el procesador genera un acceso de memoria la MMU:

1. Realiza una búsqueda de un mapeo para la dirección virtual solicitada sea seguro o no en la instrucción relevante o Micro TLB.
2. Si el paso uno falla se realiza una búsqueda de asignación para la dirección virtual solicitada sea seguro o no en el TLB principal.

De no encontrarse ninguna asignación global o asignación para el ASID seleccionado actualmente o bien no se encuentra ninguna coincidencia para la dirección virtual en el TLB, el hardware lleva a cabo una *translation table walk* de manera automática lo que devuelve al procesador un error de traducción de sección.

Si se encuentra una entrada de TLB correspondiente, la información que contiene se utiliza de a siguiente manera.

1. Los bits de permiso de acceso y el dominio se utilizan para determinar si el acceso está permitido. Si el acceso no está permitido, la MMU indica que la memoria se cancela, de lo contrario, se habilita el acceso para continuar.
2. Los atributos de la región de memoria controlan el caché y el búfer de escritura, y determinan si el acceso es seguro o no protegido en caché, no almacenado o en el dispositivo.
3. La dirección física se utiliza para cualquier acceso a memoria externa o bien acoplada para realizar la coincidencia de etiquetas para las entradas de caché.

**Habilitando y deshabilitando la MMU.**

La MMU puede ser habilitada o deshabilitada escribiendo en le bit M, para lograr esto se escribe un 0 en el registro de control CP15 c1. Al reiniciar este bit se borrará a cero deshabilitando la MMU. Este bit, además de la mayoría de los parámetros de control de MMU, se duplica como seguro y no seguro, para garantizar una política de administración de memoria clara y distinta. Para habilitar la MMU se desactivan las instrucciones de caché y después se escribe un 0 en el registro de control CP15.

**Control de acceso a memoria.**

El acceso a la región de memoria es controlado por:

**Dominios.**

Un dominio es un conjunto de regiones de memoria. Proporcionan un soporte para sistemas operativos multiusuario. Todas las regiones de memoria tienen un dominio asociado.

Es el principal mecanismo de control de acceso para una región de memoria y define las condiciones para las cuales la memoria es accedida. El dominio determina si:

* Los permisos de acceso se usan para calificar el acceso.
* El acceso está incondicionalmente permitido para proceder.
* El acceso es abortado incondicionalmente.

En los últimos dos casos los atributos de acceso de permiso son ignorados.

**Permisos de acceso.**

Los bits de permiso de acceso controlan el acceso a la región de memoria correspondiente. Si se realiza un acceso a un área de memoria sin los permisos necesarios, se genera un error de permiso. Los permisos de acceso se determinan mediante una combinación de los bits AP y APX en la tabla de páginas, y los bits S y R en el Registro de control CP15 c1.

No es necesario limpiar el TLB para permitir que los nuevos bits S y R entren en vigencia. Los permisos de acceso de las entradas en el TLB se ven automáticamente afectados por los nuevos valores S y R.

# Trabajos citados

ARM Infocenter. (Noviembre de 2009). *http://infocenter.arm.com/help/index.jsp.* Obtenido de http://infocenter.arm.com/help/topic/com.arm.doc.ddi0333h/ddi0333h\_arm1176jzs\_r0p7\_trm.pdf