CSC-640

Computer System Organization and Programming

Topic: Intel VT-d

Sheng Kai Liao

American University 4400 Massachusetts Ave, NW

Spring 2021

Intel VT-d

Introduction

Following the time, CPU architecture has various designed in hardware and software. However, due to the rise of software applications, computers more and more often interact with other computers that may not necessarily have the same hardware design. Thus, it is essential to find a standard operation environment which allow a fixed hardware design to operate different software. Nevertheless, the first thing we faced is technical issue about the adoption between software and hardware. Therefore, the virtualization technology in the CPU architecture achieves this goal by creating a virtual environment for the software, so that it can run on hardware that may not be suitable for the design. And till now, virtualization has been widely used in many aspects such as server operating and management, cybersecurity, cloud computing and so on.

To operate different software, the computer generally creates a virtual environment as called VM (Virtual Machine) which can operate different software, such as Linux, macOS or Window. The VM is usually operated by VMM (virtual machine monitor or visualizer), which is an emulator as a platform to manage different VMs' setting, such as assigned disk size, assigned I/O device and the memory size.

Also, to bridge the communication between the software and hardware, the computer translates the virtual address from CPU into the physical address for hardware devices by using the MMU (memory management unit) [6]. The MMU covert the virtual memory address into physical address with referring a map which can be designed as user needed, and the software can access the local hardware devices by this translation, it also called address mapping.

However, as a user, when we try to develop an application in virtual machine, we always need to consider many aspects about software, such as the security, efficiency, performance, and flexibility. For those considerations, Intel provided various virtualization technologies for their CPU architecture to cope with different situation or needed from client, user, and developers. For this paper, I will introduce you one of the Intel virtualization technologies which is Intel VT-d.

What is Intel VT-d?

Intel VT-d (Intel Virtualization Technology for Directed I/O) is a virtualization technology in x86 CPU architecture virtualization. The specific feature of Intel VT-d is that it allows user to directly assign the I/O devices for each virtual machine [2]. The virtual machine could be benefitted by such feature. Overall, the security, efficiency, and the flexibility of VM will be improved in certain area by using VT-d.

How it works

In traditional, the virtualization provides DMA (direct memory access) which allow the main memory to access I/O devices [1][4]. All actions from DMA been controlled by DMAC (direct memory access controller) which manages the interruption and operation of data translation from I/O devices to CPU. General speaking, DMA is like a method to relief the CPU work for processing the data from I/O devices. When DMAC receive the CPU instruction, it takes the responsibility to managing the process of storing data from I/O into memory. After that, when the process done, it returns an interruption call to CPU and the data location in memory as address so that CPU know that processing is done and know where to load the data [7]. However, using DMAC may cause cache coherence issue [2]. The cache coherence issue means that the caches are not synchronized, and the data will not be the same for each cache. Also, all

VMs data transmission are rely on DMA, it increases the damage by I/O attacks and therefore arise the issue about data leaking.

Intel VT-d provided direct access between PCI device and the operating VM (Virtual machine) with IOMMU (input–output memory management unit) [2]. The PCI devices will be virtualized by SRIOV (Single-root input/output virtualization) which allow signal physical PCI device to share data with VMs in virtual environment with I/O bus [8]. IOMMU is a MMU extension to I/O devices management which is able directly to access I/O bus. Same as MMU, the IOMMU translates the I/O devices virtual addresses from SRIOV into physical address for memory with a designed map [5]. In this way, VMM is able to assign the I/O devices for each VM by setting IOMMU. Furthermore, by address mapping, Intel VT-d is able to restrain DAM function in order to achieve DMA-remapping. DMA-remapping change the request from DMA into physical memory and checking the access right for VMs. In this case, DMA-remapping truly implements the isolation for DMA as a protection domain. Thus, in Intel VT-d, the system is able to create multi-DMA protection domains for VMs to isolate the DMA for different VMs, and each VM has their own I/O map for accessing local hardware.

Also, the I/O performance can be improved by the Intel VT-d. As we known, one server can run many VMs at the same time. But each operation has different demand for I/O performance. By only using DMA without I/O limitation, DMA will directly respond the request from the VMs to all available I/O devices, and this way may slow down the I/O performance. Nevertheless, in VT-d, the DMA will be limited by IOMMU. Accordingly, the users can assign the I/O resource to the high I/O demanded VM application so that I/O resource could be appropriated assigned. It can not only prevent the speed drop caused by unorganized I/O usage, but also improve the flexibility of I/O management.

Purpose

Intel VT-d improve many aspects of virtualization. There have several examples from Intel manual. For example, when you are operating multiple OS (operation system) and VMs, if one of system performing any delinquent DMA, you may encounter multiple system failure due to the DMA error. In this end, it emphasized the importance of I/O device isolation so that when the error occurred, other OS and VMs will not be affected [2].

The other example is about online server. As we know, the online server always required intensive data transmission and management by I/O devices. Therefore, the flexibility and the performance are prior consideration for online servers. To fulfill this kind of demand, Intel VT-d I/O assignment feature could help developer to organize the I/O devices for each VM on servers [2].

Last example, Intel VT-d could be used for protecting potential I/O attack and data leakage. In cybersecurity, there is a way to hack computers or servers by insert I/O devices such as USB, network card and camcorder, the attack method usually be called I/O attack or DMA attack [3]. By this way, the malicious device can place the virous into the system or just directly stole the data. Yet, by isolated I/O devices for operating VMs, it not only limited the damage from I/O attack but also targeted the breaking point for this kind of attack so that users are able to strengthen the risky area [2][3].

Conclusion

To summarize, Intel VT-d provided powerful feature for virtualization technologies. In several examples I provided above, it proofed that Intel VT-d improves the flexibility, security, performance and efficiency in many aspects of virtualization. By assigning and isolating I/O

devices for VMs, it provided a chance to users to fully manage their I/O resources as their desired. Following the constantly increased demand for virtualization, I believed that Intel VT-d can be one of your choice or alterative in someday.

Reference List

[1] UNDERSTANDING X86 VIRTUALIZATION.

Link: https://mixstersite.wordpress.com/2019/11/12/understanding-x86-virtualization/#:~:text=The%20VMM%20provides%20an%20emulated,is%20built%20for%20x86%20hardware.

[2] Intel® Virtualization Technology for Directed I/O (VT-d): Enhancing Intel platforms for efficient virtualization of I/O devices.

Link: https://software.intel.com/content/www/us/en/develop/articles/intel-virtualization-technology-for-directed-io-vt-d-enhancing-intel-platforms-for-efficient-virtualization-of-io-devices.html?wapkw=vt-d

[3] Morgan, B. & Alata, É. & Nicomette, V. & Kaâniche, M. (2018). IOMMU protection against I/O attacks: a vulnerability and a proof of concept. *Journal of the Brazilian Computer Society volume.* Link: https://link.springer.com/article/10.1186/s13173-017-0066-7

[4] What Does Direct Memory Access (DMA) Mean?

Link:https://www.techopedia.com/definition/2767/direct-memory-access-dma

[5] IOMMU introduction

Link:https://terenceli.github.io/%E6%8A%80%E6%9C%AF/2019/08/04/iommu-introduction

[6] Memory management unit – Wikipedia

Link: https://en.wikipedia.org/wiki/Memory_management_unit

[7] How does a DMA controller work?

Link: https://softwareengineering.stackexchange.com/questions/272470/how-does-a-dma-controller-work

[8] CHAPTER 13. SR-IOV

Link: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/virtualization_host_configuration_and_guest_installation_guide/chap-virtualization_host_configuration_and_guest_installation_guide-sr_iov