Investigating effects of hardware isolation in high-speed network environments

Simon Ellmann
advised by Paul Emmerich, Florian Wiedner, Benedikt Jaeger

Monday 23rd November, 2020

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

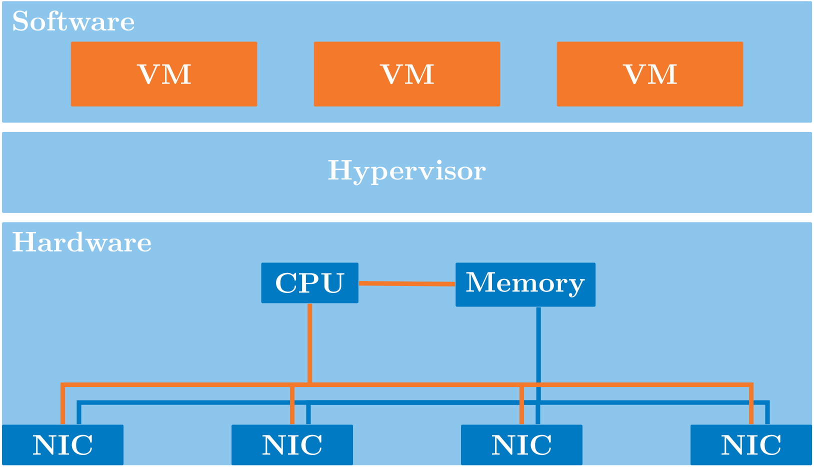
Introduction

What is hardware isolation?

Limiting access of software and hardware to needed resources

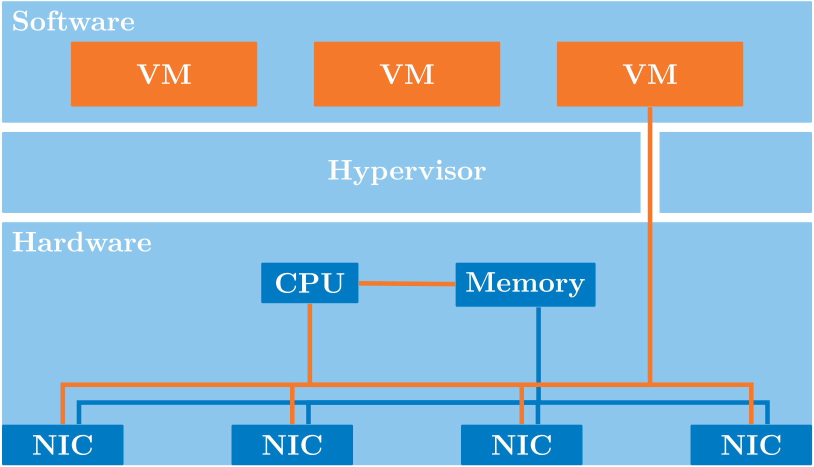
Introduction

Why hardware isolation?



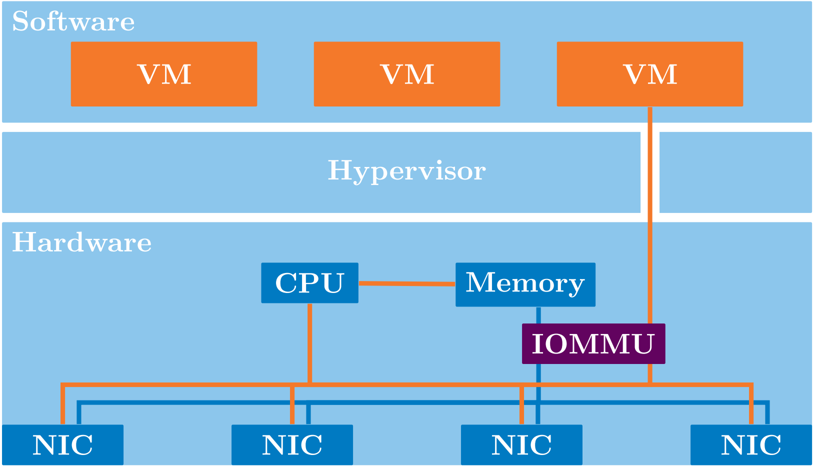
Introduction

Why hardware isolation?



Introduction

Why hardware isolation?



Introduction

Hardware isolation via the IOMMU

Input-Output-Memory-Management-Unit (IOMMU):

- translates IO virtual addresses (IOVA) to physical addresses (PA)

Advantages:

- limits effects of faulty or malicious devices/software by restricting memory access
- contiguous address space does not have to be contiguous in physical memory
- enables 32-bit devices to address memory above 4 GiB

Use cases:

- virtualization
- vital when connecting untrusted devices via PCIe, Thunderbolt, ...

Introduction

Why should we look at the IOMMU?

Reasons to have a closer look:

- not that much information available about IOMMU implementations
- some publications report huge performance impacts and vulnerabilities
- implementation differences between vendors (Intel, AMD, ...) mostly unknown

Key question:

- What is the trade-off between performance and safety/security?

Effects of the IOMMU

Performance impact

- in non-virtualized and
- virtualized environments

Effects of the IOMMU

Performance impact: Test setup

Performance measured with ixy.rs:

- state-of-the-art user space network driver
- can forward >26 million $\frac{\text{packets}}{\text{s}}$ on a single 3.3 GHZ CPU core
- less than 2,000 lines of code
- written in Rust

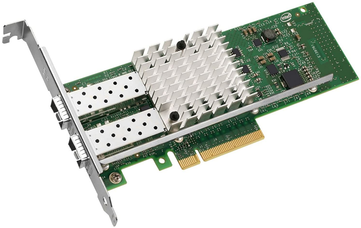
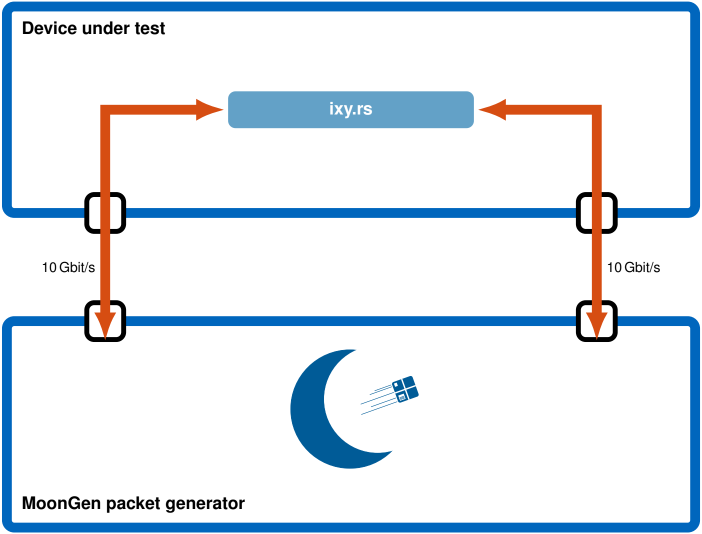


Figure 1: Intel X520-DA2 [Picture: amazon.com]

Effects of the IOMMU

Performance impact: Test setup



Effects of the IOMMU

Performance impact: Test setup

Model	Clock rate	Cores	Released
Intel Xeon E3-1230 v2	3.3 GHz	4	2012
Intel Xeon E5-2620 v3	2.4 GHz	6	2014
AMD EPYC 7551P	2.0 GHz	32	2017

Table 1: CPU models of device(s) under test

Effects of the IOMMU

Performance impact: Baseline

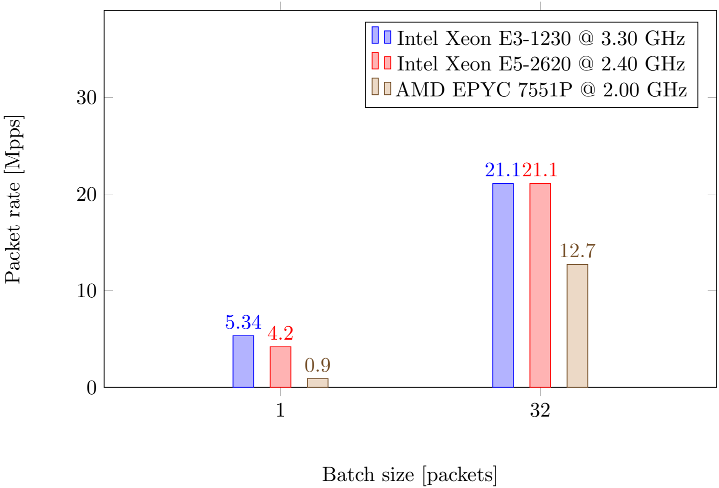


Figure 2: Single core forwarding rate of CPUs with different batch sizes, no IOMMU.

Effects of the IOMMU

Performance impact: Non-virtualized environments

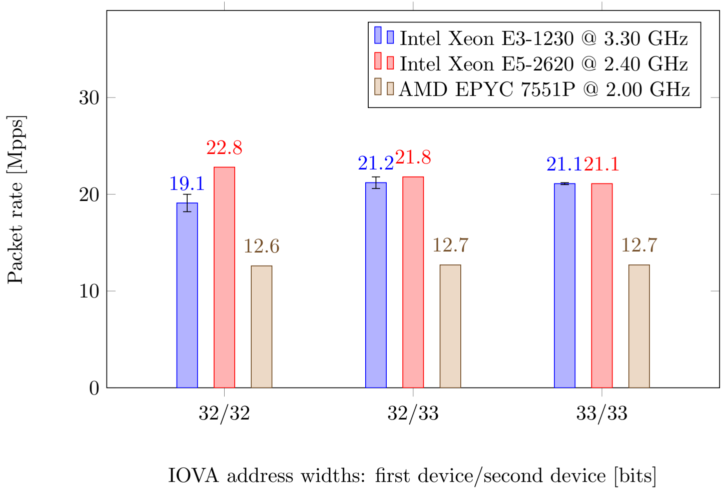


Figure 3: Forwarding rate with 32 to 33 bit wide IO virtual addresses.

Effects of the IOMMU

Performance impact: Non-virtualized environments

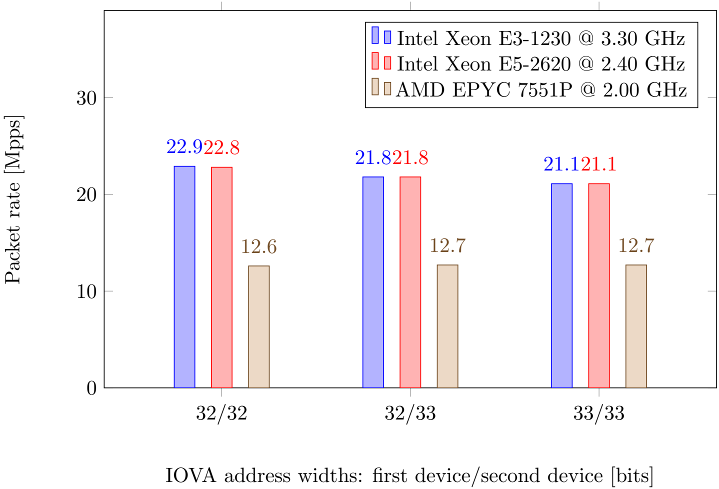


Figure 4: Forwarding rate with 32 to 33 bit wide IO virtual addresses, replacing the mem-pool's free-stack by a queue.

Effects of the IOMMU

Performance impact: Non-virtualized environments

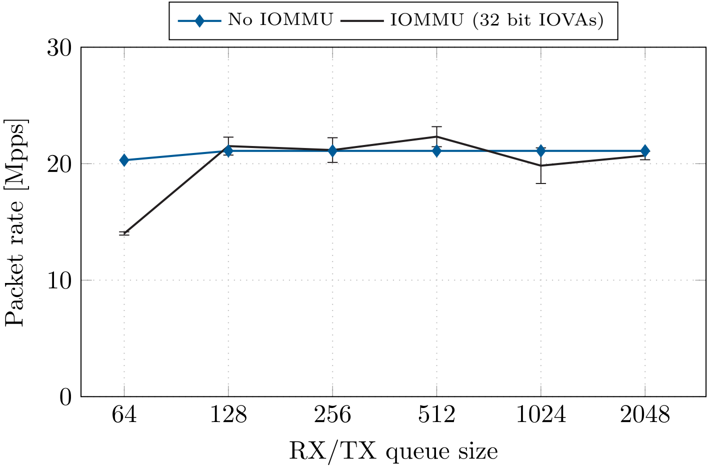


Figure 5: Forwarding rate of Intel Xeon E3-1230 v2 with different RX/TX queue sizes.

Effects of the IOMMU

Performance impact: Non-virtualized environments

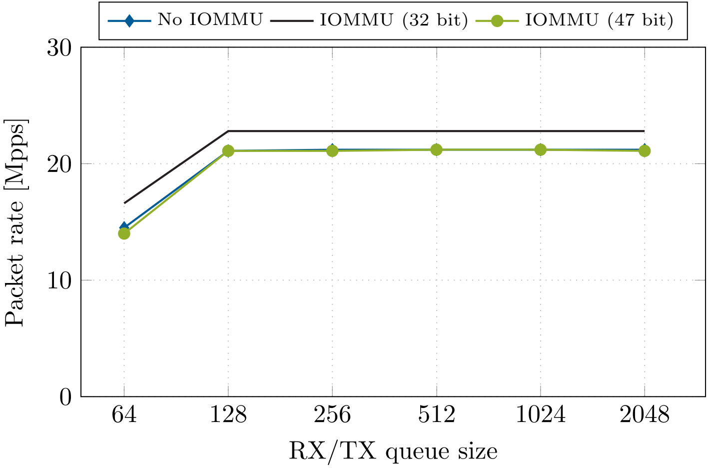


Figure 6: Forwarding rate of Intel Xeon E5-2620 v3 with different RX/TX queue sizes.

Effects of the IOMMU

Performance impact: Non-virtualized environments

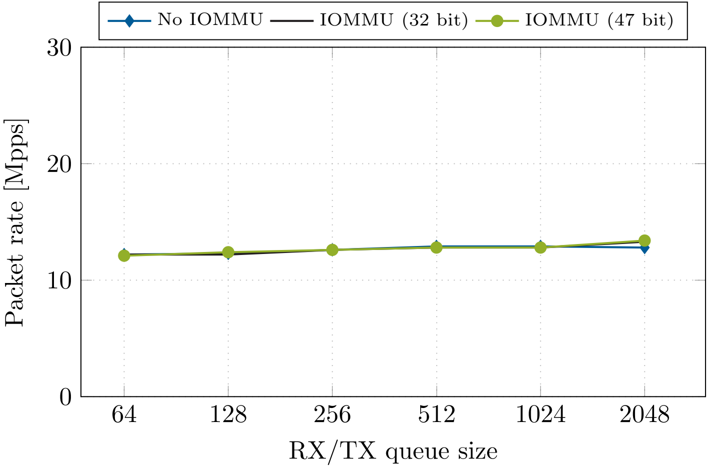


Figure 7: Forwarding rate of AMD EPYC 7551P with different RX/TX queue sizes.

Effects of the IOMMU

Performance impact: Non-virtualized environments

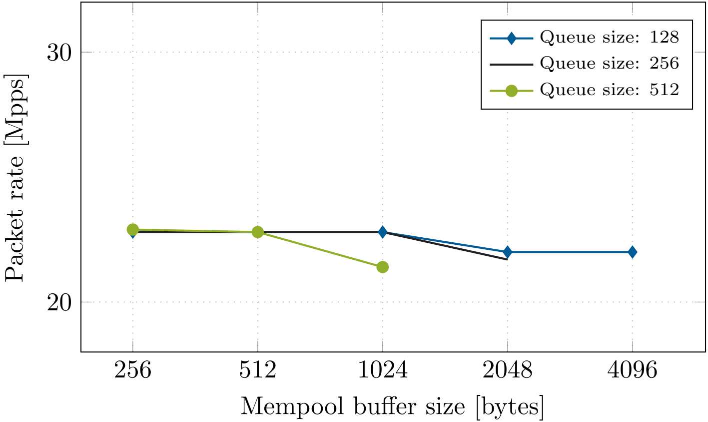


Figure 8: Forwarding rate of Intel Xeon E3-1230 v2 with 4 KB pages and various queue/buffer sizes.

Effects of the IOMMU

Performance impact: Non-virtualized environments

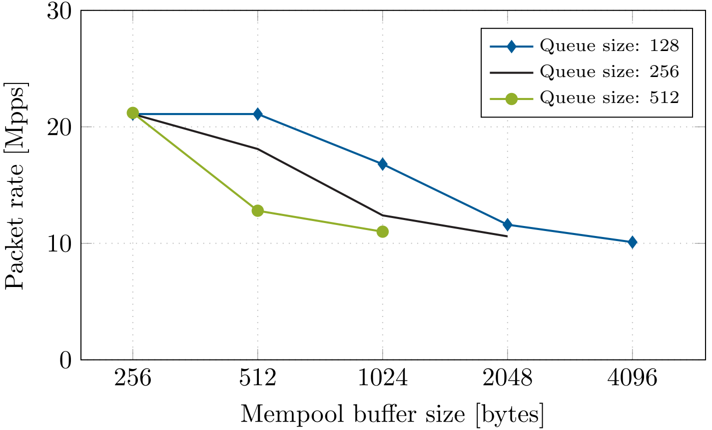


Figure 9: Forwarding rate of Intel Xeon E5-2620 v3 with 4 KB pages and various queue/buffer sizes.

Effects of the IOMMU

Performance impact: Non-virtualized environments

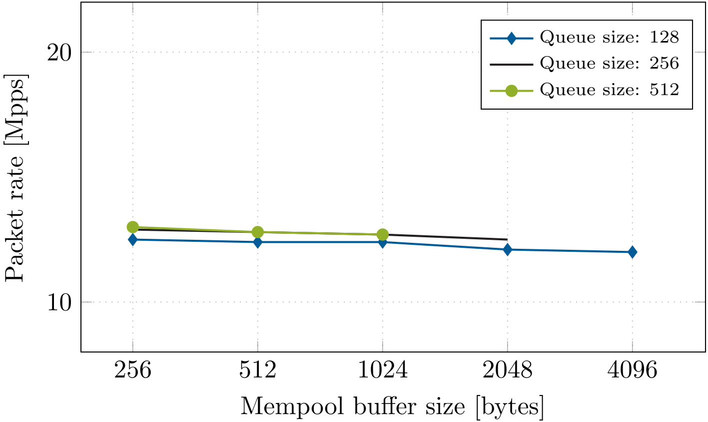


Figure 10: Forwarding rate of AMD EPYC 7551P with 4 KB pages and various queue/buffer sizes.

Effects of the IOMMU

Performance impact: Non-virtualized environments – Summary

IOMMUs may improve performance ...

- in PCIe-bottlenecked networks by using shorter (e.g. 32 bit) IO virtual addresses

IOMMUs may cause performance degradation ...

- when the IO-TLB gets thrashed

Effects of the IOMMU

Performance impact: Virtualized environments

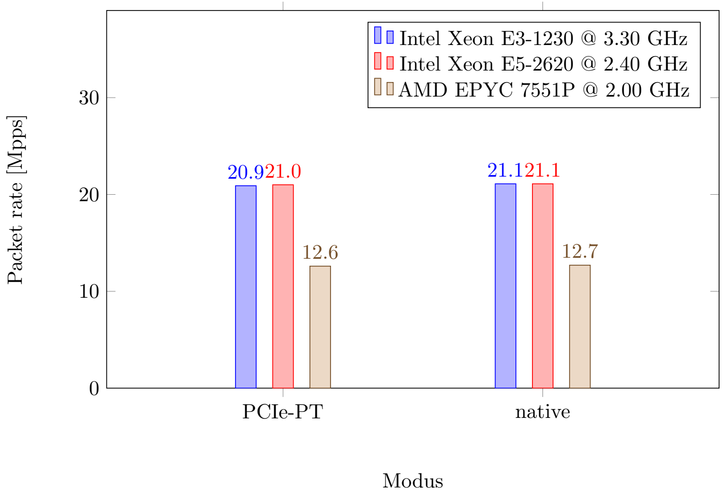


Figure 11: Forwarding rate using PCIe passthrough vs. native.

Remaining research questions

Performance impact: Virtualized environments

To be continued

Remaining research questions

- Does the IOMMU impact performance of SR-IOV or virtual switches?
- Are IO-TLB entries shared between multiple devices?
- Does the IO-TLB affect security on virtualized systems?