Full Packet Capturing

in 10 Gigabit Network

By Panuwach Boonyasup
Supervise by Dr. Takano Ryousei, Asst. prof Vasaka Visoottiviseth
In part of AIST and MUICT cooperation

Objective

“Implement full packet packets capturing in 10 Gbps wire-rate by reducing bottleneck within packet capturing process”

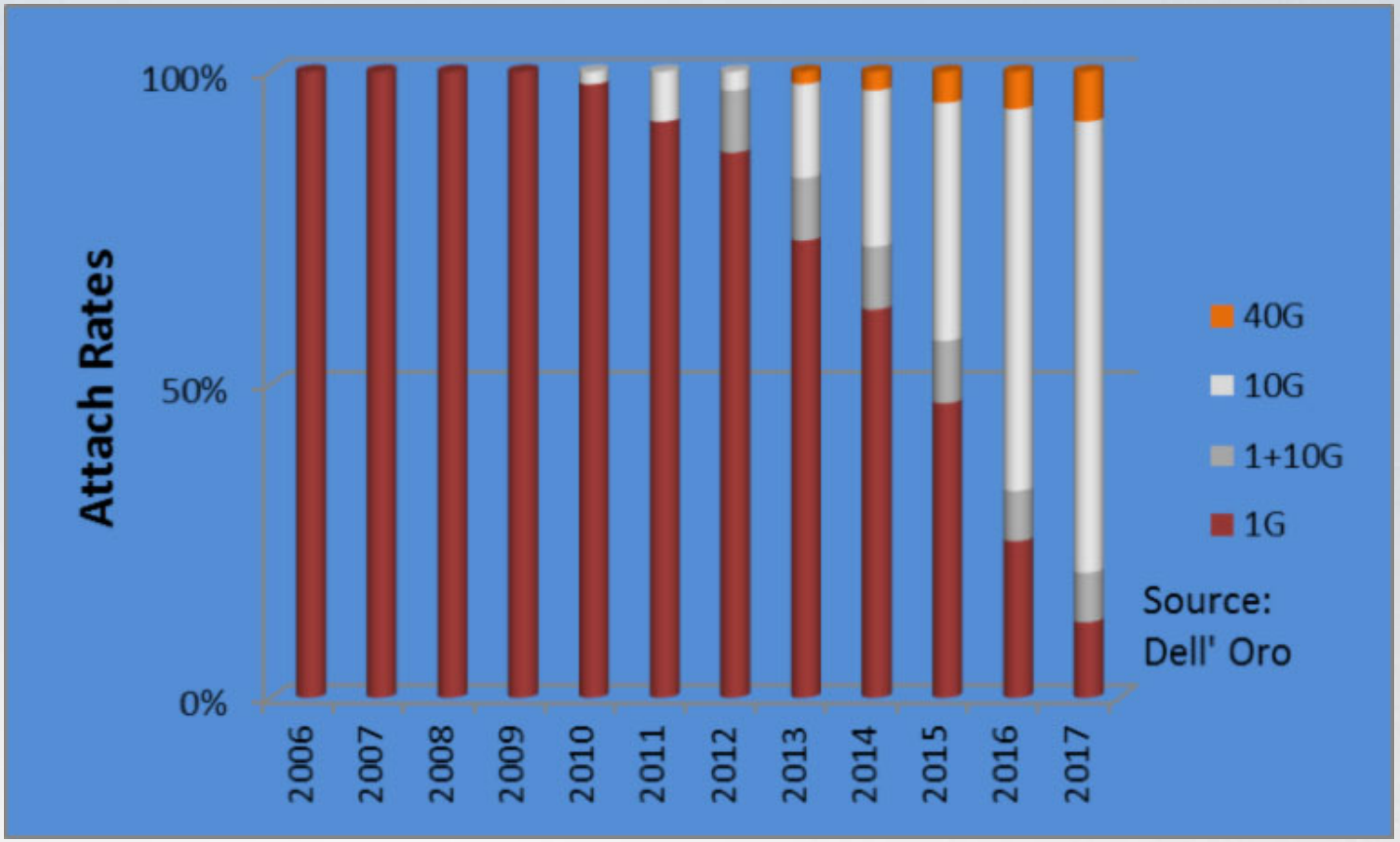
Background and Contribution

Why full packet capturing?

- It gives advantage to network security analysis in term of flexibility and granularity

Why 10 Gbps wire-rate?

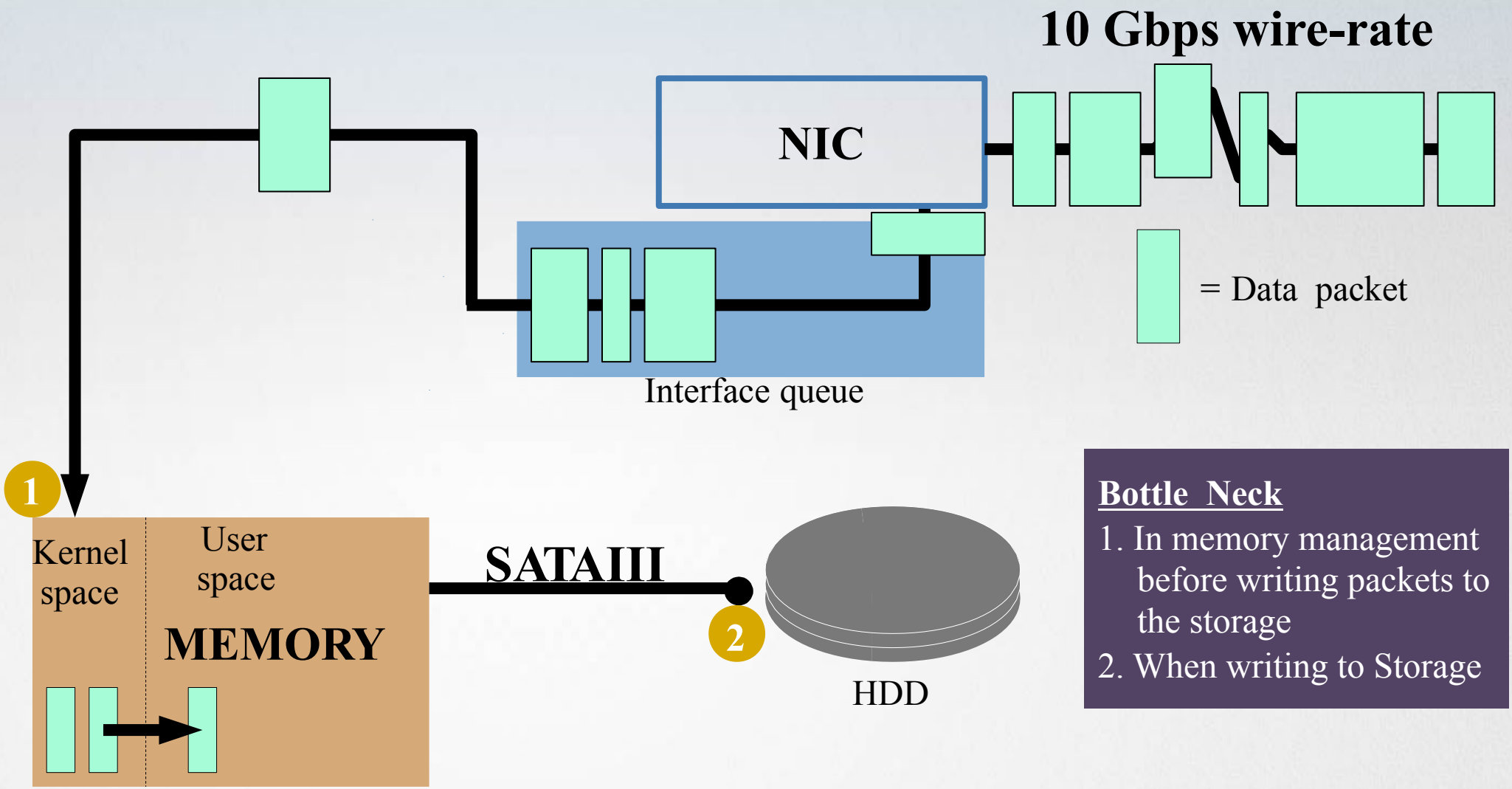
- It is a trend that 10 Gbps Ethernet market share is increasing continuously



O'Reilly, J. (2014, 1 22). *Will 2014 Be The Year Of 10 Gigabit Ethernet?* Retrieved 5 9, 2016, from Networkcomputing: http://www.networkcomputing.com/networking/will-2014-be-year-10-gigabit-ethernet/1076051359

Intel. (n.d.). *New Trends Make 10 Gigabit Ethernet.* Retrieved 9 4, 2016, from Intek: http://www.intel.com/content/dam/support/us/en/documents/network/sb/intel_neutral_10gbe_wp_v6.pdf

Scope of Problems



Bottle Neck

1. In memory management before writing packets to the storage
2. When writing to Storage

Solutions Design

Bottle neck: **in memory management before writing packets to the storage**

DPDK :

Allow user get access to hardware such as memory, NIC and CPU directly bypassing kernel by various DPDK's library.

- **Use DPDKCap as packet capturing tool**

  : DPDKCap implement LZO compression for saving storage space

LZ4 :

Faster compression algorithm than LZO, has lower compression ratio as a trade-off.

Solutions Design

Bottle neck: when writing to Storage

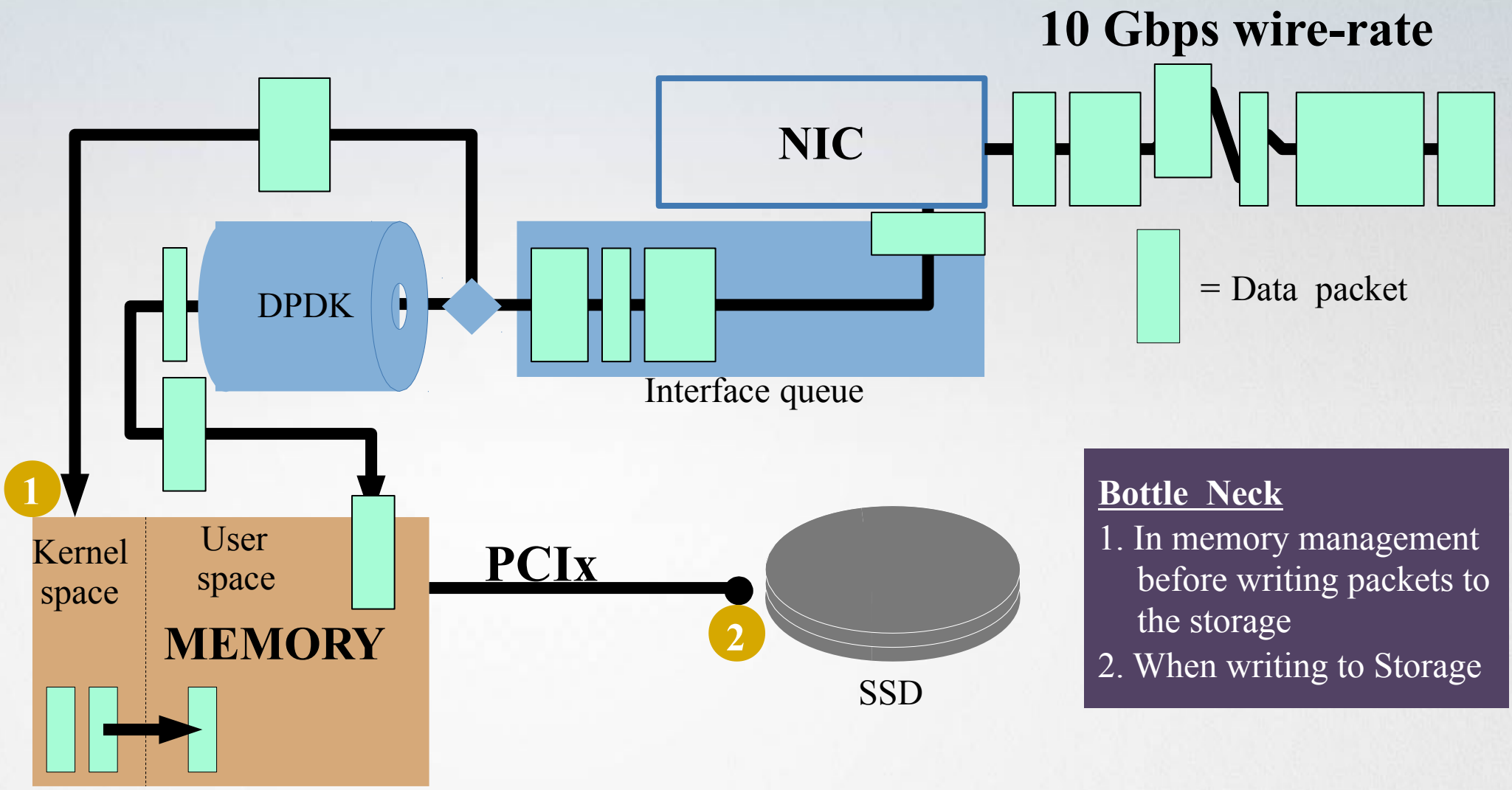
SSD (Solid State Drive) :

Use SSD with write rate of 2.2 GB/s instead of HDD which will increase maximum write rate

Multi-core Writing :

Writing with Multi-core that provided by DPDK library allow faster in write speed

Solutions Design



Bottle Neck

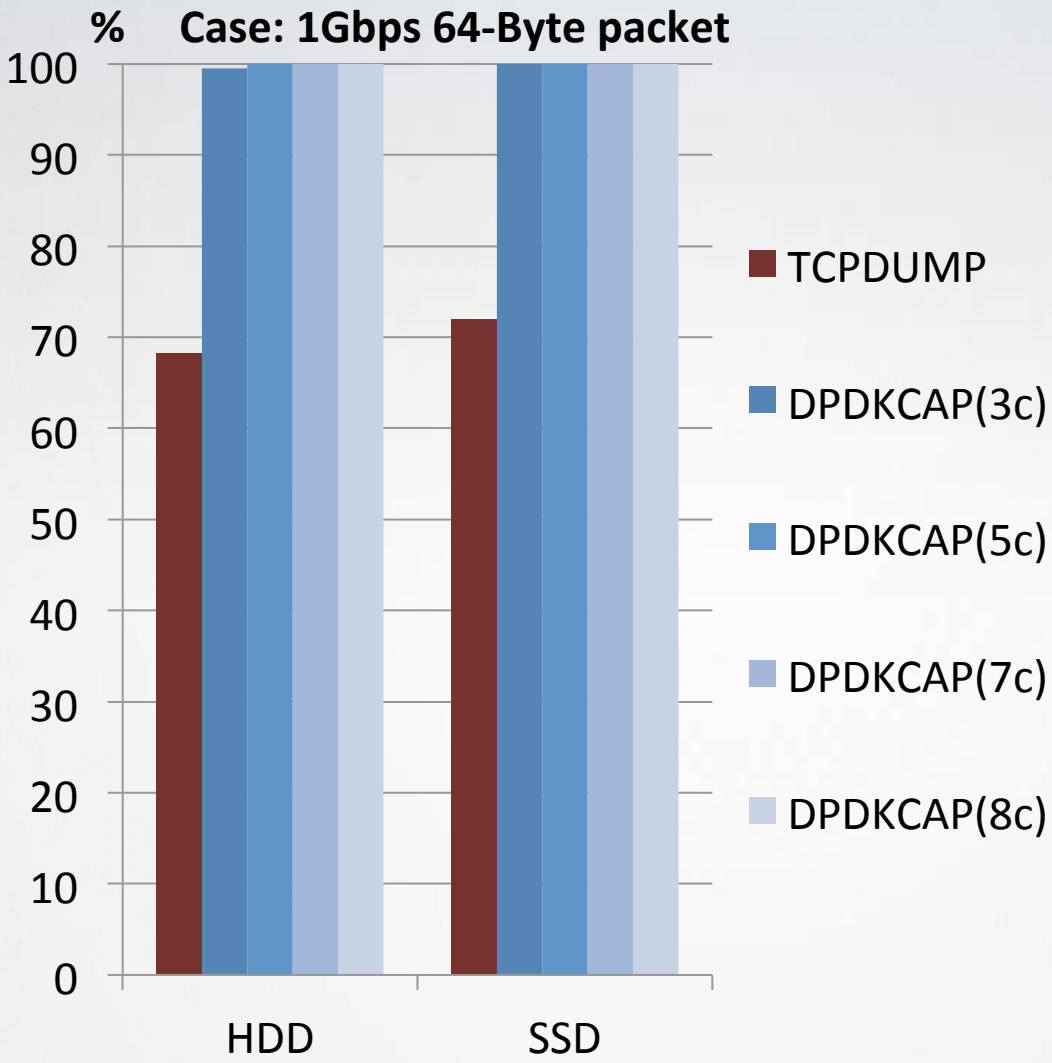
1. In memory management before writing packets to the storage
2. When writing to Storage

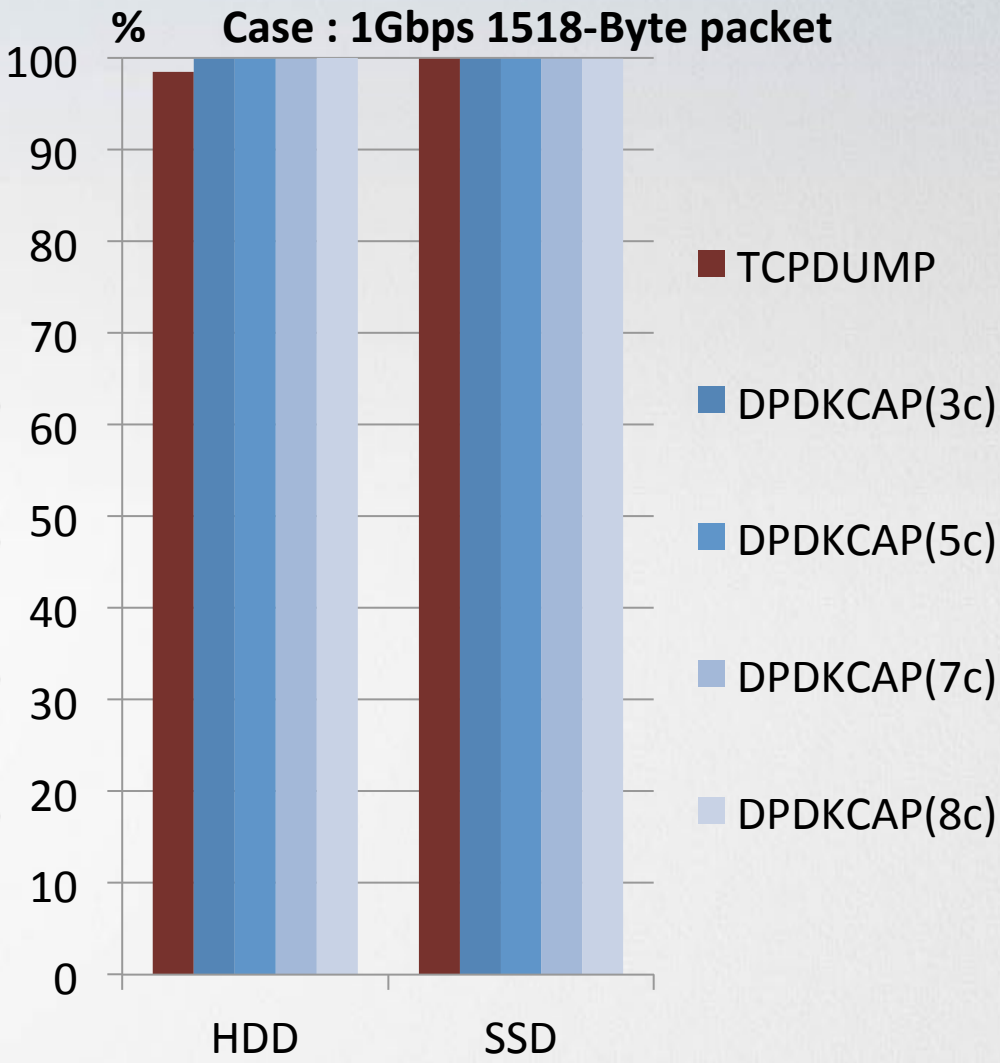
Solution Implementation

Tcpdump	• Kernel-based **packet capturing tool** • Frequently use as network diagnostic tool • Provide multiple function in many layer that increase its utility like listening on specific interface or specific ip address.
DPDKCap	• DPDK base **packet capturing tool** • Implement compression technique to increase its performance. • Can make use of multi-core environment
Moongen	• A DPDK base **packet generating tool** using lua script as the method to control packet generating • Can make use of multi-thread in packet generating Can control content of packet

Implementation Result

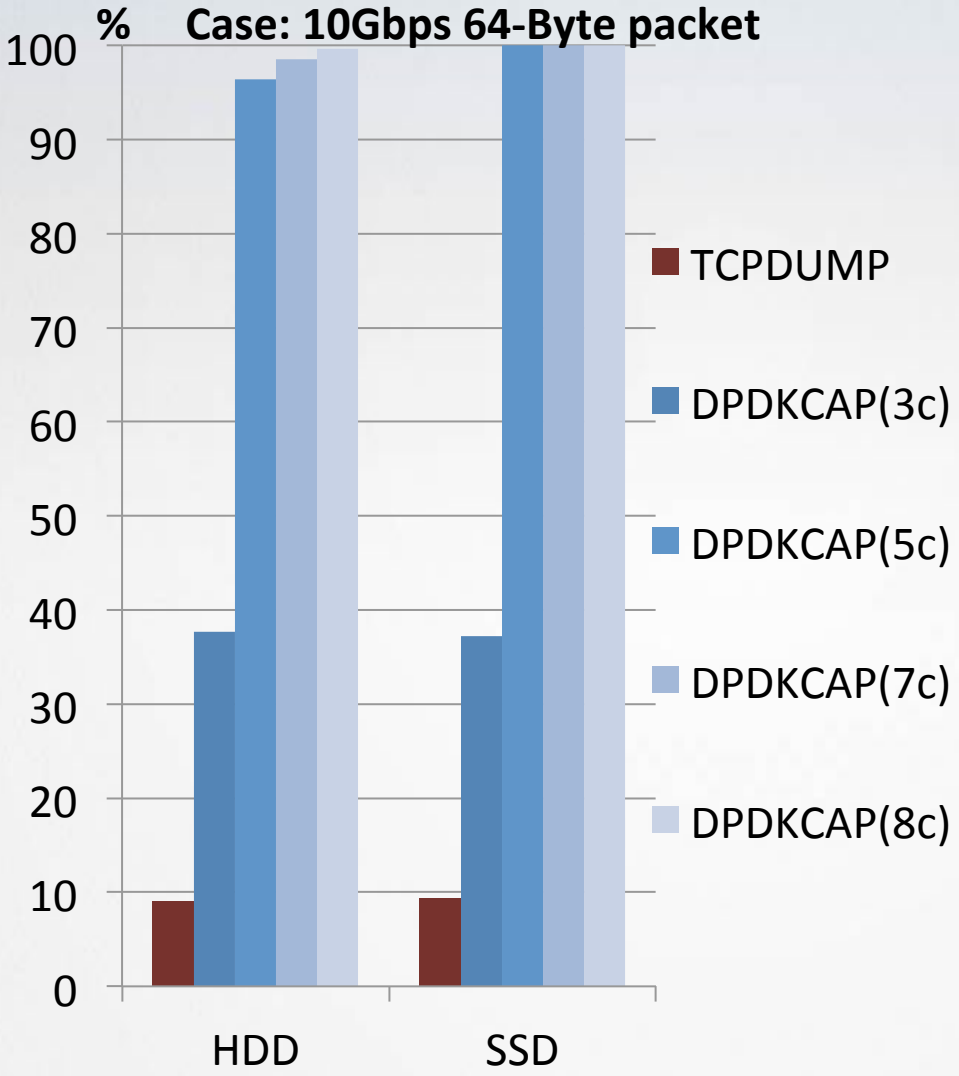
Packet success in percentage compare SSD,HDD and Multi-core 1 Gbps environments

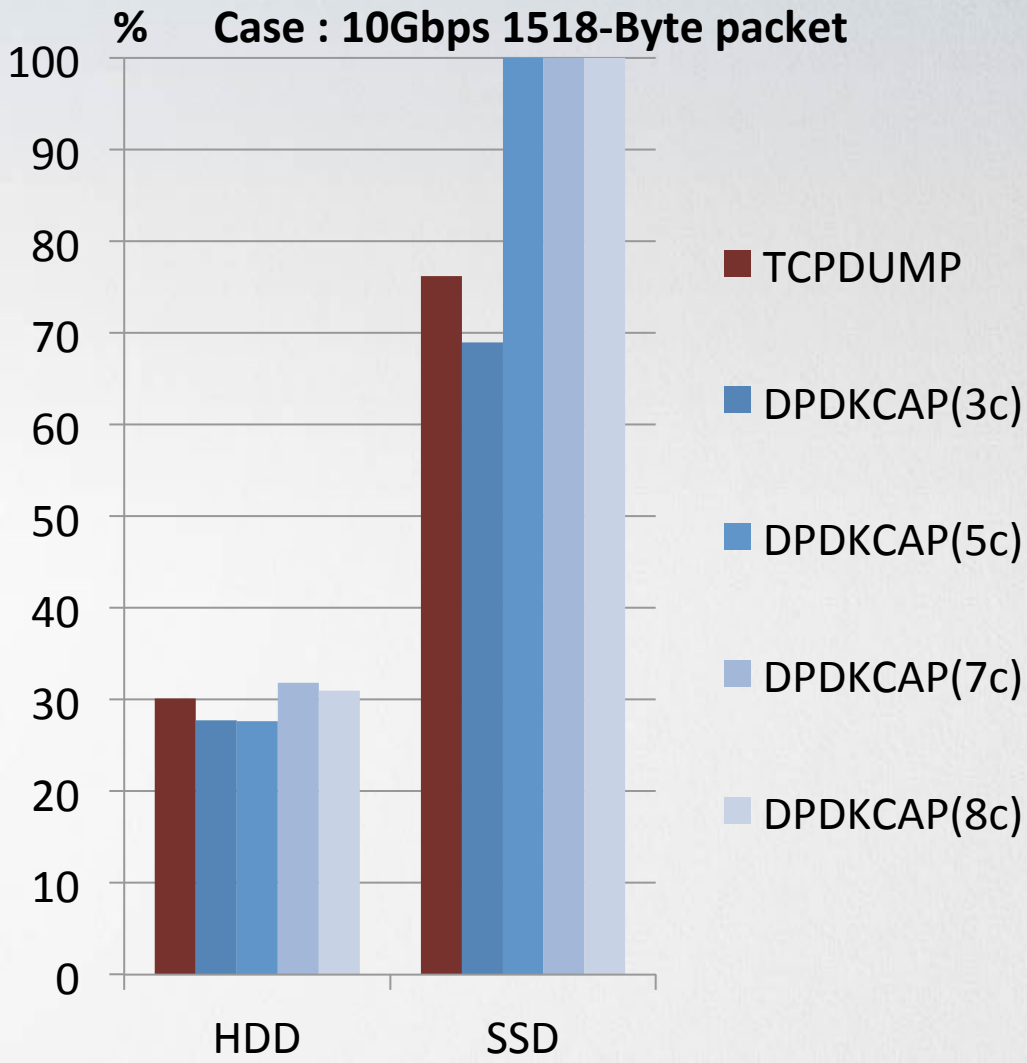




Implementation Result

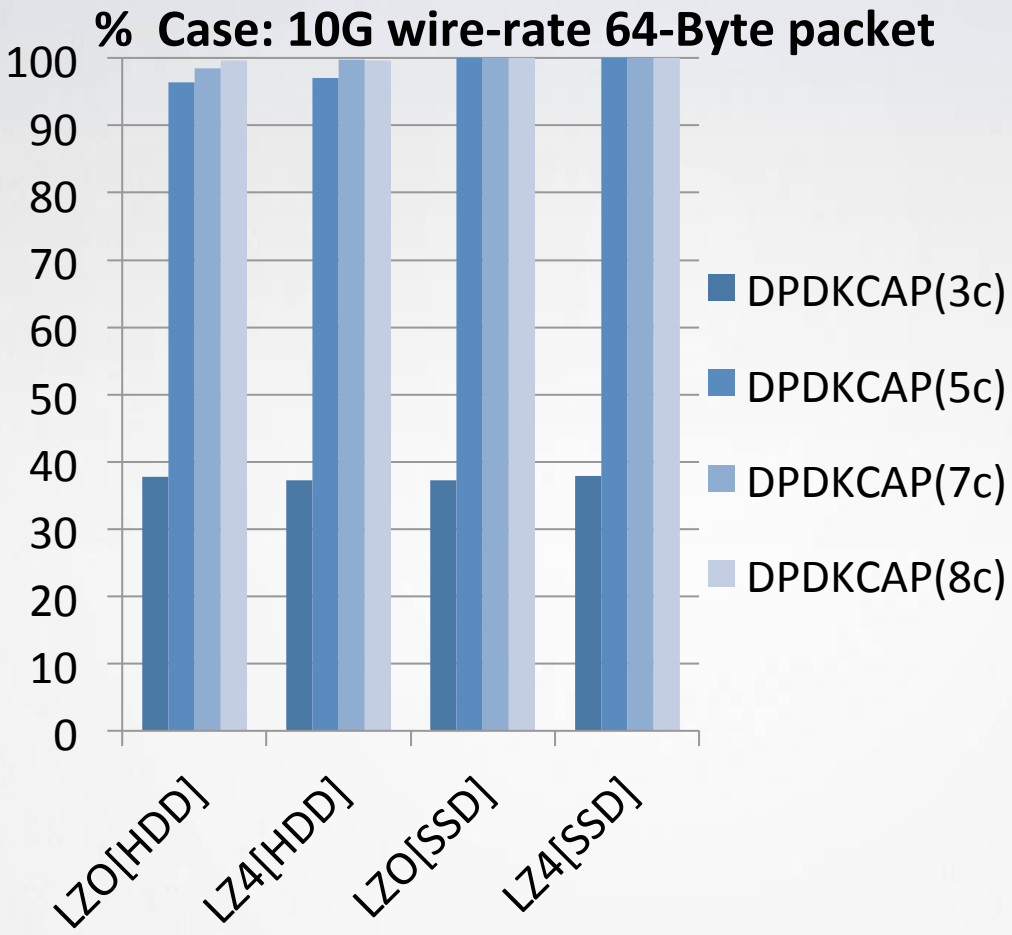
Packet success in percentage compare SSD,HDD and Multi-core 10 Gbps environments

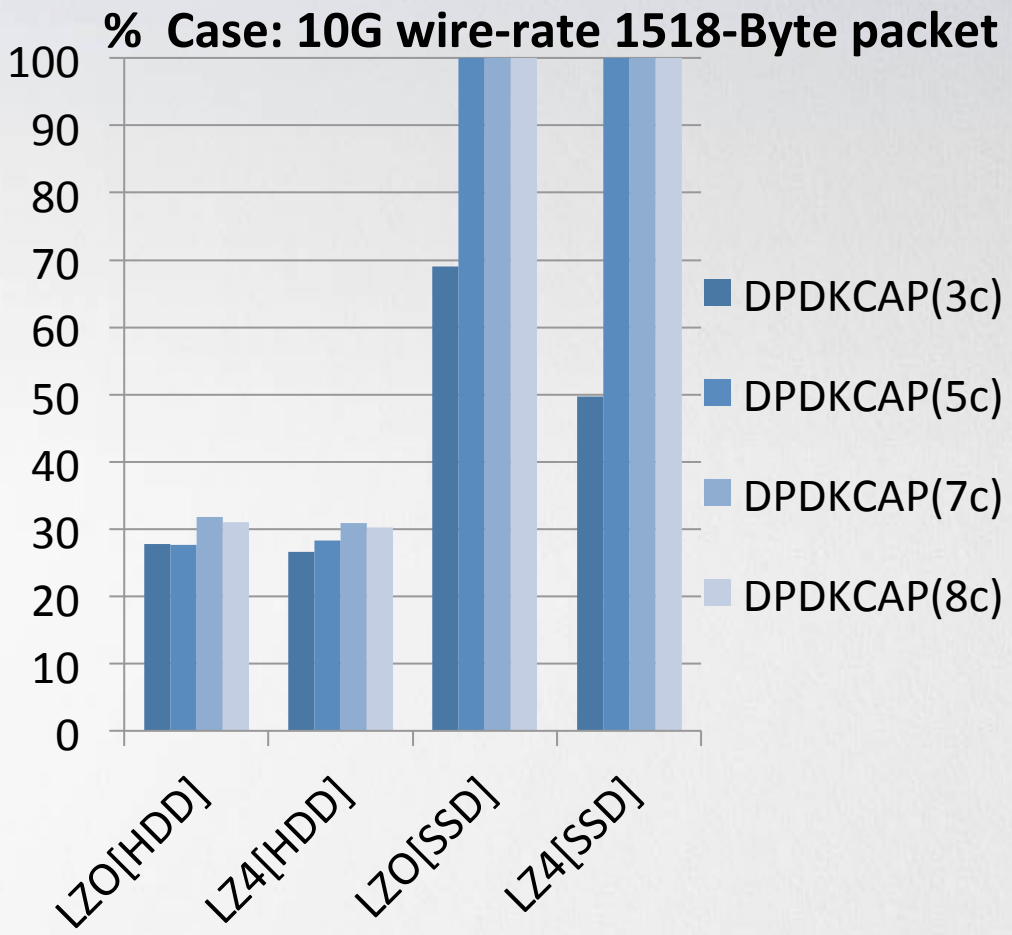




Implementation Result

Result of packet capturing with LZO compression compare to LZ4





Conclusion

- DPDKCap have better performance than TCP-DUMP
- Multi-core packet writing allows faster packet capturing
- With SSD and multi-core writing we can Achieve the full packet capturing in 10Gbit wire-rate in off-the-shelf hardware.

References

[1] “DPDK website”, http://dpdk.org, visited on 28/07/2016
[2] “DPDKCAP git website”, https://github.com/Woutifier/dpdkcap, visited on 28/07/2016
[3] “DPDK-Replay git website”, https://github.com/marty90/DPDK-Replay, visited on 28/07/2016
[4] “Moongen website”, https://github.com/emmericp/MoonGen, visited on 28/07/2016 [5] “LZ4 website”, https://github.com/Cyan4973/lz4, visited on 28/07/2016
[6] “MAWI Working Group Traffic Archive”, http://mawi.wide.ad.jp/mawi/, visited on 28/07/2016
[7] “TaoSecurity”, http://taosecurity.blogspot.com/2012/11/why-collect-full-content-data.html, visited on 9/6/2016