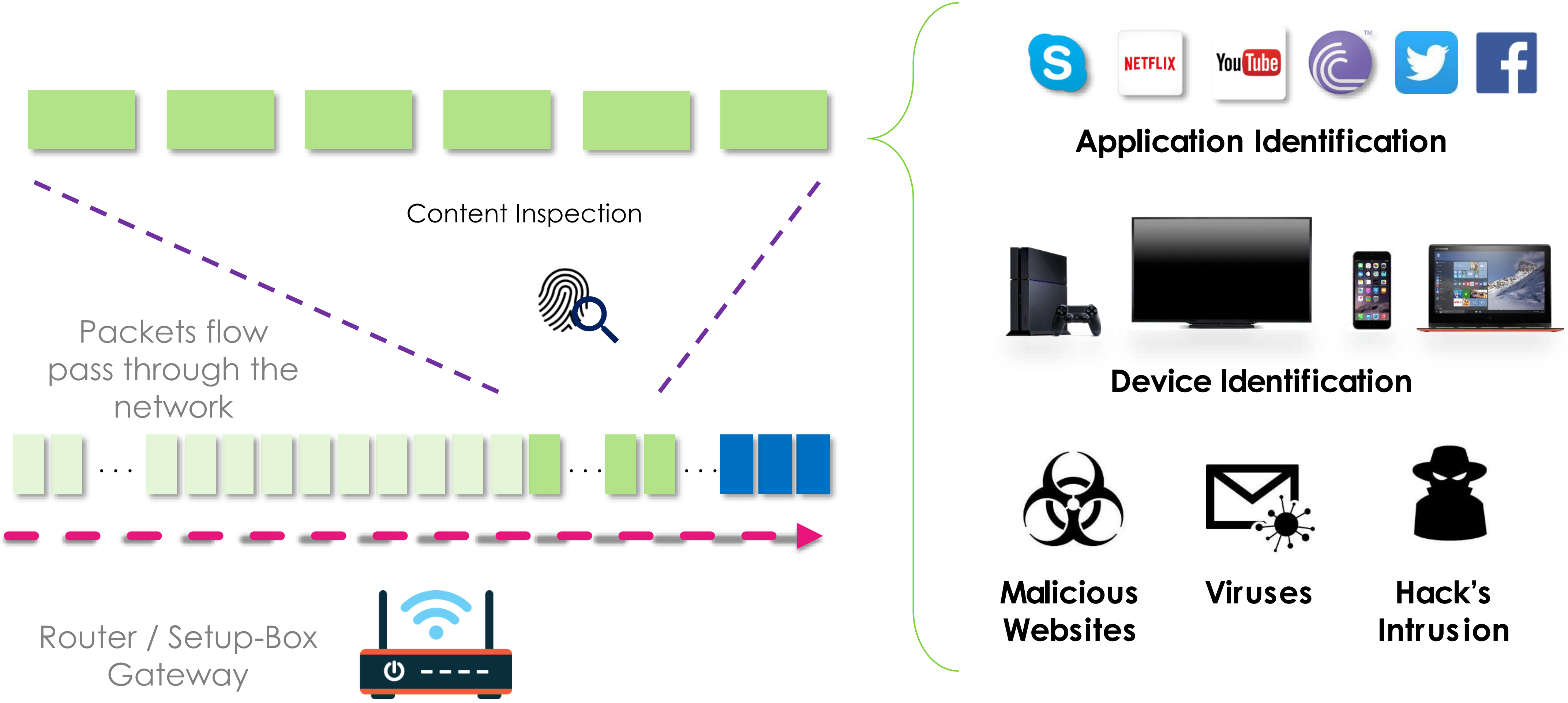
DPDK
DATA PLANE DEVELOPMENT KIT

Multiple vDPI Functions using DPDK and Hyperscan on OVS-DPDK Platform

Cheng-Chien SU
Fang-Chen KUO
LIONIC Corp.

What is **Deep Packets Inspection**?



Content Inspection

Packets flow pass through the network

Router / Setup-Box Gateway

Application Identification

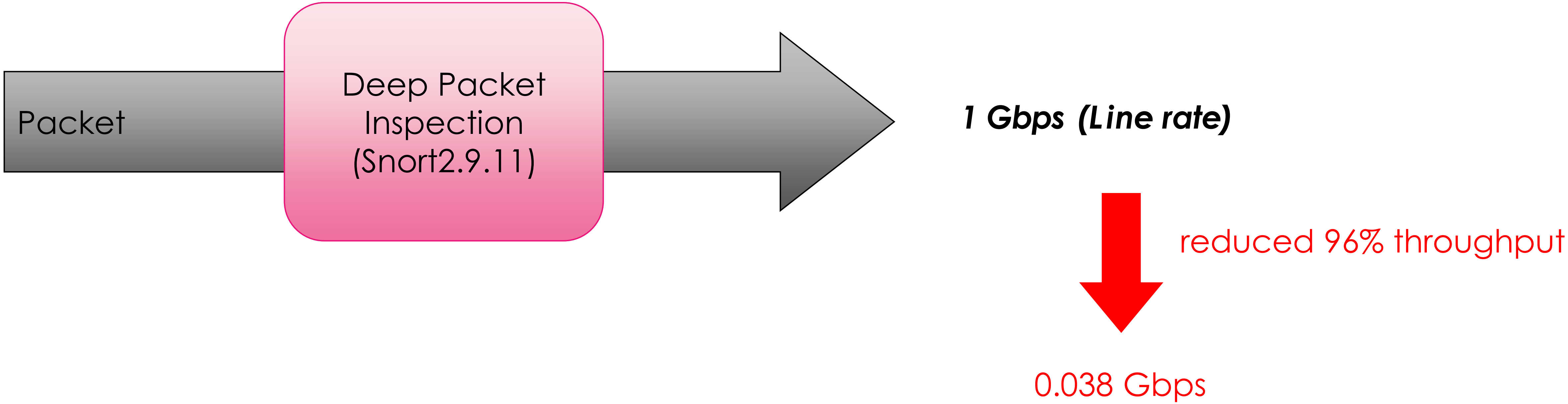
Device Identification

Malicious Websites

Viruses

Hack's Intrusion

Deep Packet Inspection Problem



Packet

Deep Packet Inspection (Snort2.9.11)

1 Gbps (Line rate)

reduced 96% throughput

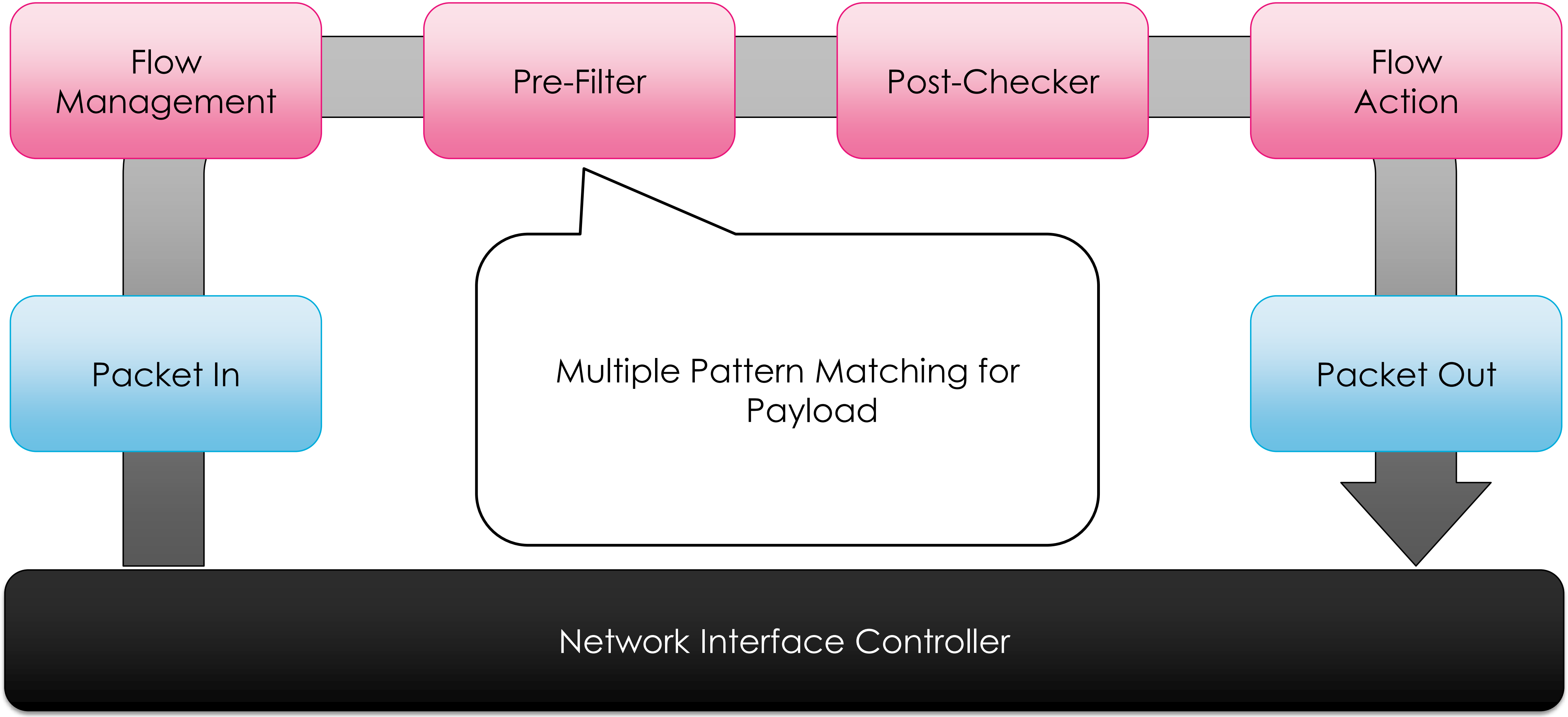
0.038 Gbps

Note: Intel Atom C3958 Platform

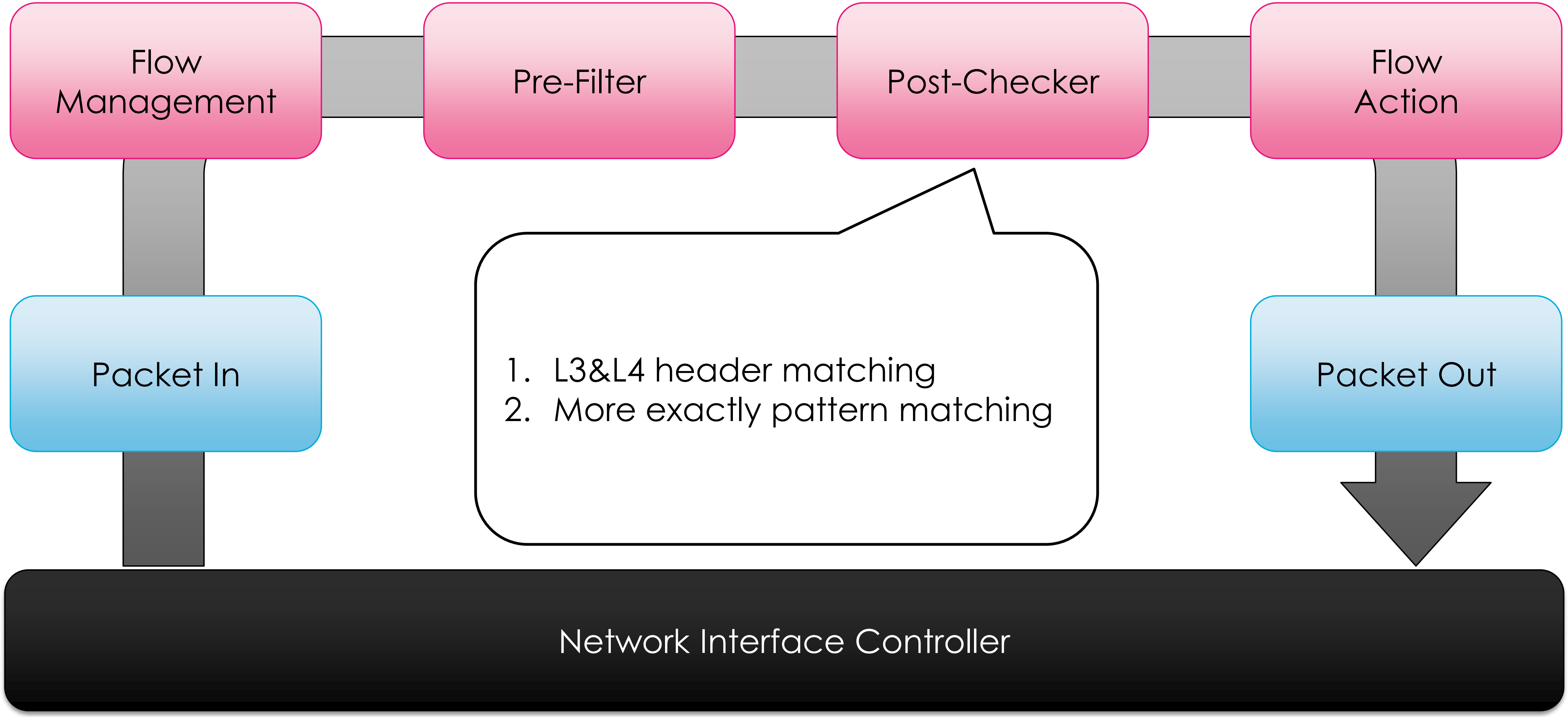
Agenda

- DPI Workflow
- How to improvement DPI throughput in Intel Platform
  - DPDK
  - Hyperscan
  - Content Merging
- Multiple vDPI Function on OVS-DPDK Platform
- Throughput Comparison

DPI Workflow (1/2)

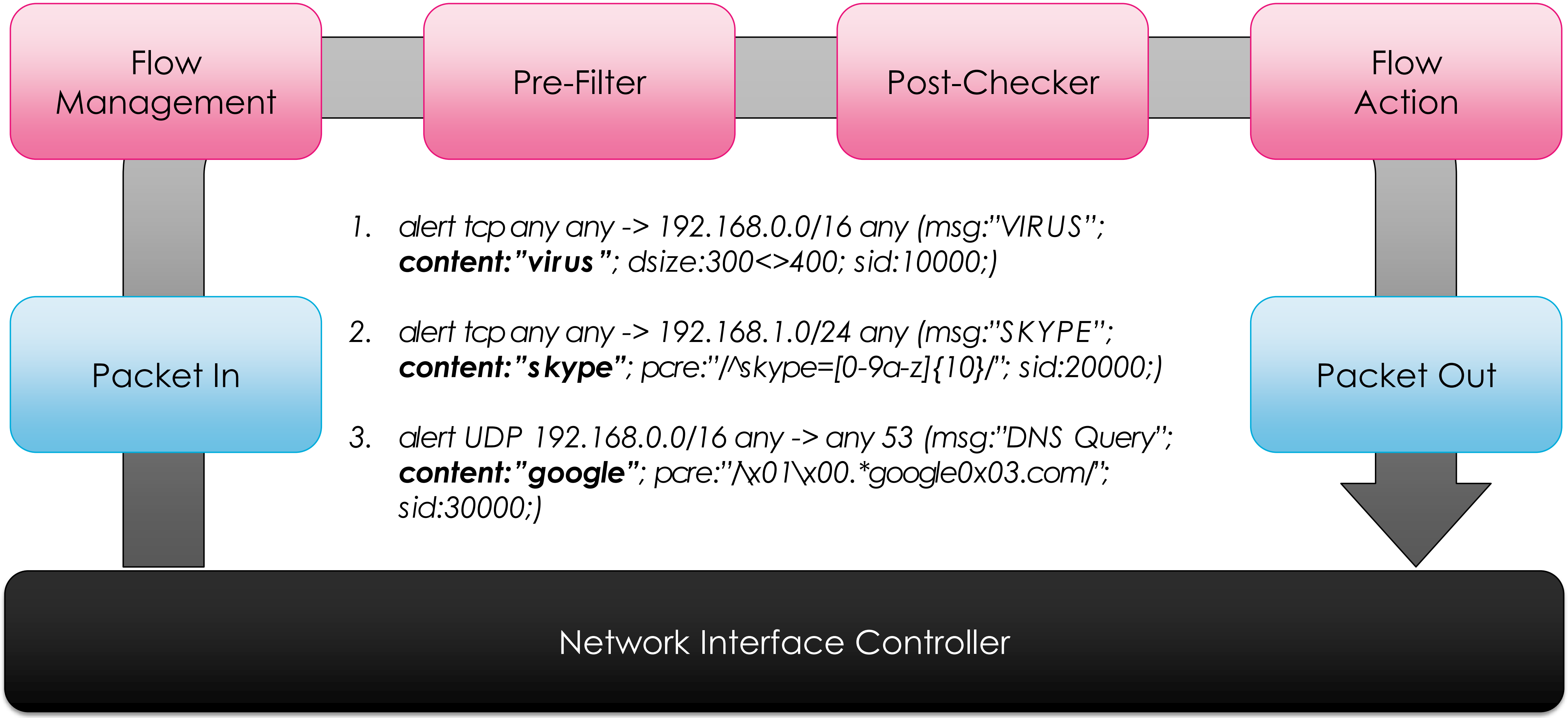


DPI Workflow (2/2)



1. L3&L4 header matching
2. More exactly pattern matching

DPI - Example

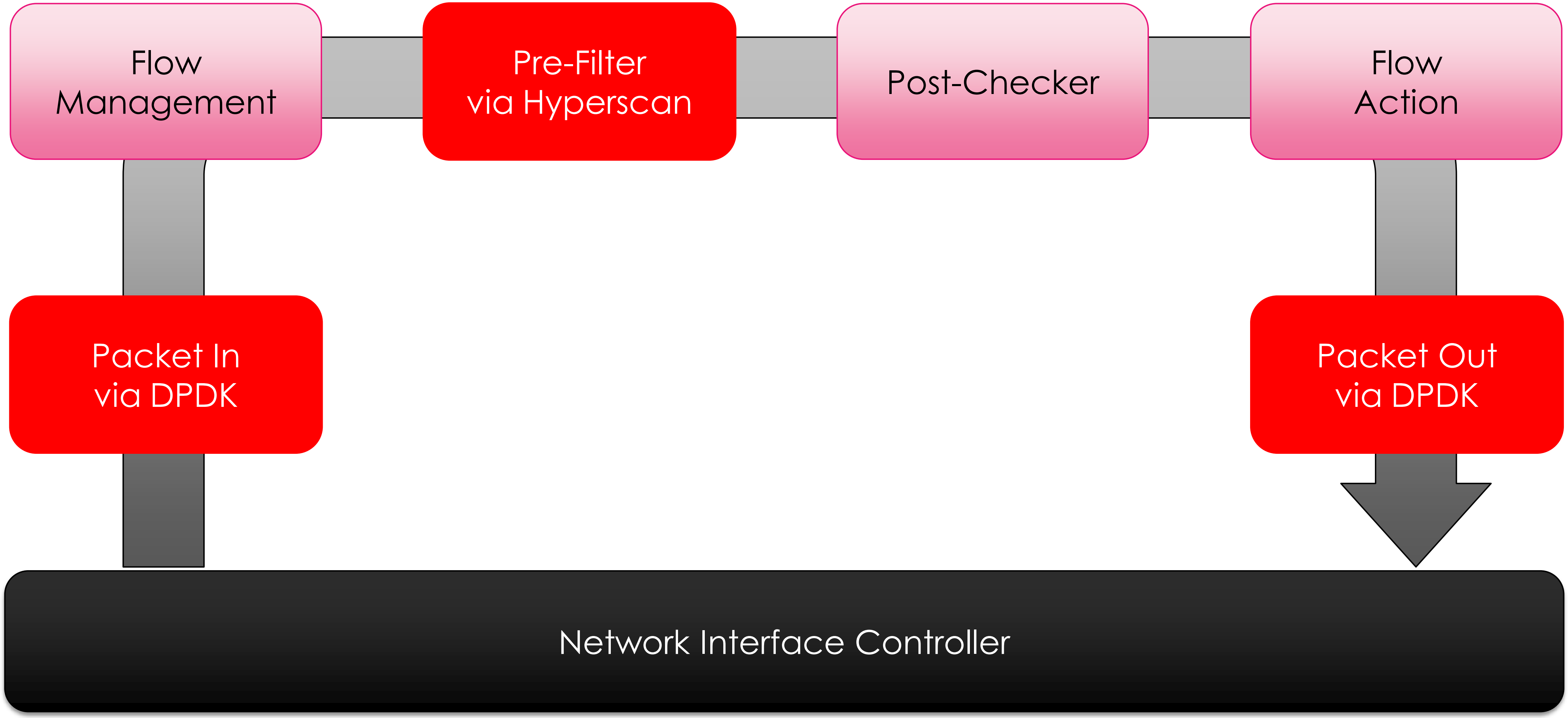


1. alert tcp any any -> 192.168.0.0/16 any (msg:”VIRUS”; **content:”virus ”**; dsize:300<>400; sid:10000;)

2. alert tcp any any -> 192.168.1.0/24 any (msg:”SKYPE”; **content:”skype”**; pcre:”/^skype=[0-9a-z]{10}/”; sid:20000;)

3. alert UDP 192.168.0.0/16 any -> any 53 (msg:”DNS Query”; **content:”google”**; pcre:”/\x01\x00.*google0x03.com/”; sid:30000;)

How to improvement DPI throughput in Intel Platform



Content Merging (1/2)

- Pre-filter support regular expression
- Increase the complexity of pattern to reduce the number of post check
- Compatible with snort format

Content Merging (2/2)

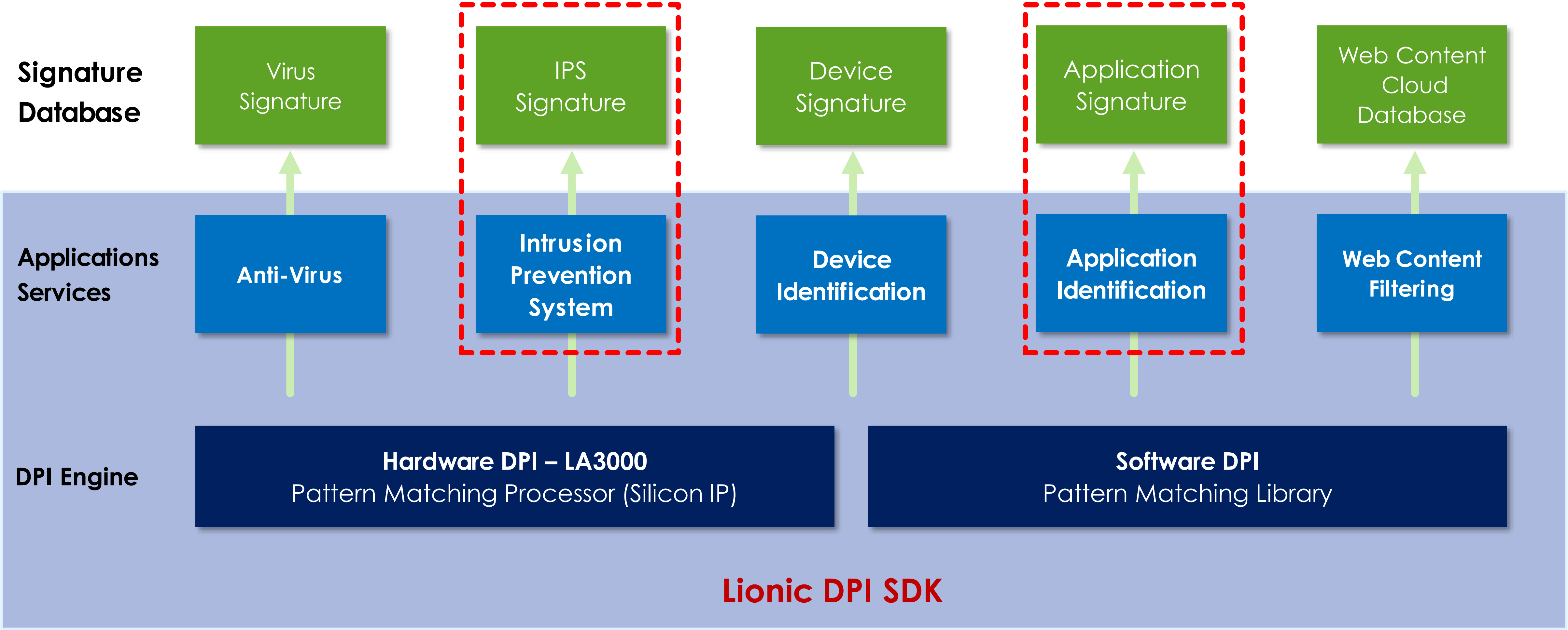
- alert tcp $EXTERNAL_NET any -> $HOME_NET any (content:"|12 01|"; **content:"|01 00 00 00|"**; within:5; distance:2;)

- Pattern: “**\x01\x00\x00\x00**”
- Regular Expression: “**\x12\x01.{2,3}\x01\x00\x00\x00**”

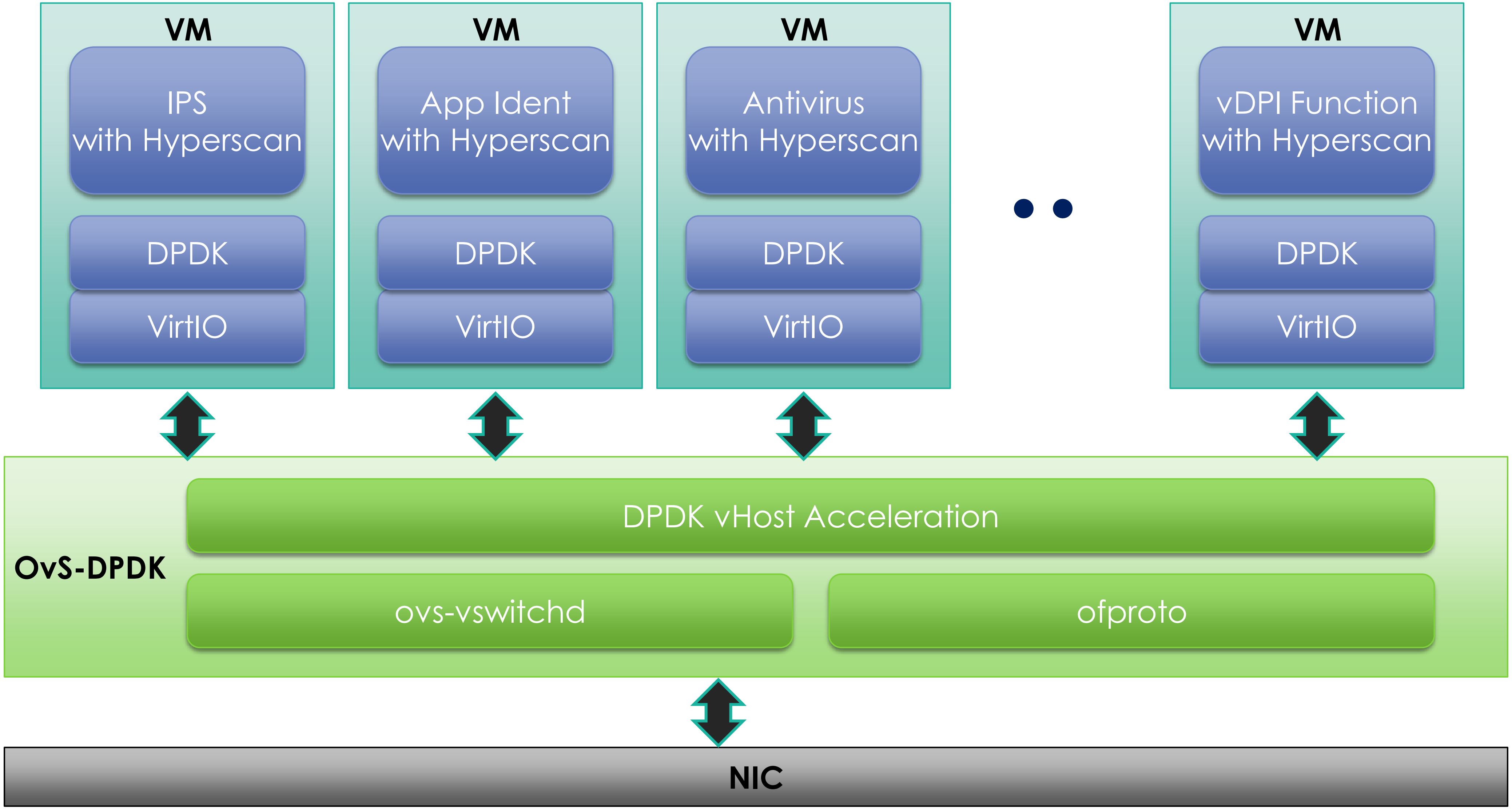
Lionic DPI SDK (1/2)

- Lionic DPI-SDK provide antivirus, intrusion prevention system, application identification, device identification and web content filtering.
- Lionic DPI-SDK is compatible with snort rule format.
- Lionic DPI-SDK supports DPDK and Hyperscan.

Lionic DPI SDK (2/2)



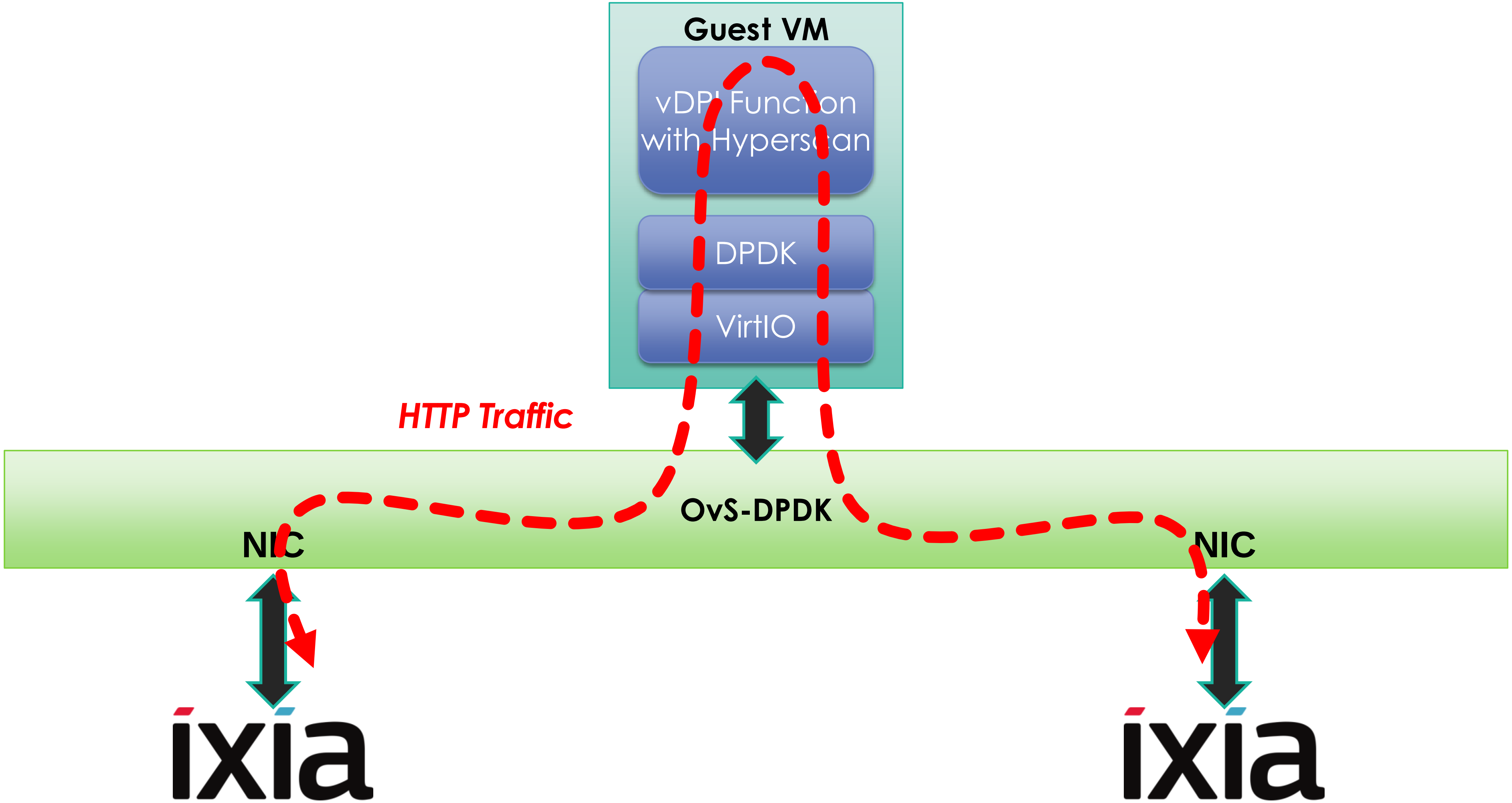
Multiple vDPI Function on OVS-DPDK Platform



Test Platform Specification

- **Hardware** – NEXCOM vDNA 1160
  - Intel Atom C3958 SoC 16 cores @ 2GHz
  - **Memory**: 32GB
  - **NIC**: Intel i350 AM4 1GbE*4, Marvell PHY 1GbE*2
- **OS**: Debian 9.4
- **OvS** version: 2.9.0
- **DPDK** version: 18.02.1
- **Hyperscan** version: 4.7.0
- **Snort** Version: 2.9.11
- All the VMs are created by KVM and emulated by QEMU
- Run IXIA IxLoad (version 3.30.58.17) on the provided environment

Test Environment



Throughput Comparison

vDPI Function	Throughput (Mbps)	Impact
No inter-VM	872.29	0%
Snort (NFQ, Aho-Corasick)	38.71	96%
Snort (NFQ, Hyperscan)	95.84	89%
Snort (DPDK, Hyperscan)	269.39	69%
Lionic-IPS (DPDK, Hyperscan)	795.02	9%
Lionic-App_Ident (DPDK, Hyperscan)	864.77	1%

Note: IPS rules are 9791, App_Ident rules are1858

Snort Resource

- Snort access packets via DAQ module
  - Patch for DAQ-2.0.6 available at:
    - http://seclists.org/snort/2016/q2/385
    - Follows the instruction on the page to build Snort with patched DAQ module
- Snort 2.9.x does not support using Hyperscan as MPSE
  - Patch for Snort 2.9.8.2 are available at:
    - https://01.org/zh/downloads/hyperscan-integration-snort-2.9.8.2-and-2.9.9.0?langredirect=1
  - Some modification based on the patch to support Snort 2.9.11.1

DPDK
DATA PLANE DEVELOPMENT KIT

THANK YOU!

LIONIC

arthur.su@lionic.com

kuo.kuo@lionic.com