OPEN POSSIBILITIES.

Using Open Interfaces to Advance AI/ML for Networking

OCP GLOBAL SUMMIT

NOVEMBER 9-10, 2021

Using Open Interfaces to Advance AI/ML for Networking

Gidi Navon
Senior Principal System Architect, Marvell

MARVELL™

OPEN POSSIBILITIES.

OPEN COMMUNITY®

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Overview

Company founded
1995

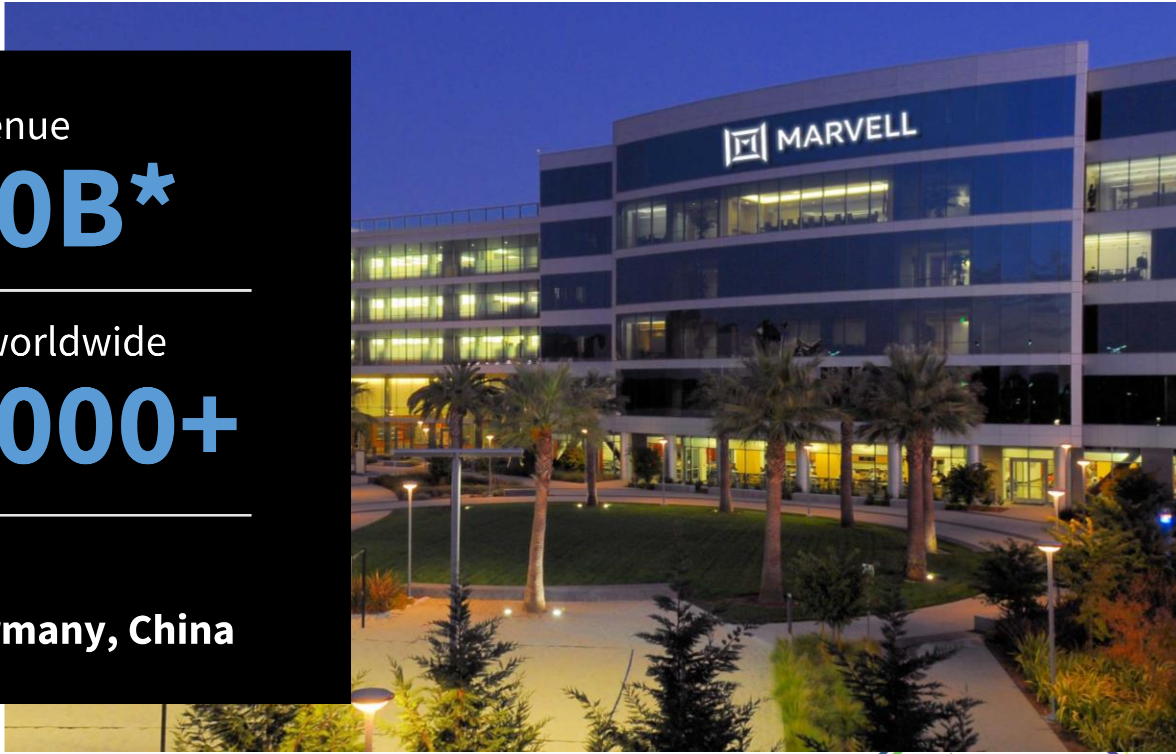
FY21 revenue
$3.0B*

Employees
6,000+

Patents worldwide
10,000+

Located in **Santa Clara, CA**

R&D centers in **US, Israel, India, Germany, China**



*Excludes Inphi CY2020 revenues ($0.68B)

Industry-leading data infrastructure product lines

Compute

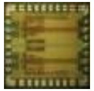
Data Processor Units (DPUs)

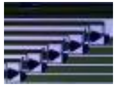
SmartNICs

Security Solutions

Networking

High-speed Electro-Optics (PAM4 DSPs, Coherent DSPs, TIAs, Drivers and Silicon Photonics)





Ethernet PHYs

Ethernet switches

DCI optical modules

Automotive ethernet

Storage

HDD controllers and pre-amps

Flash SSD controllers and NVMe accelerators

Fibre Channel HBAs

Custom ASICs

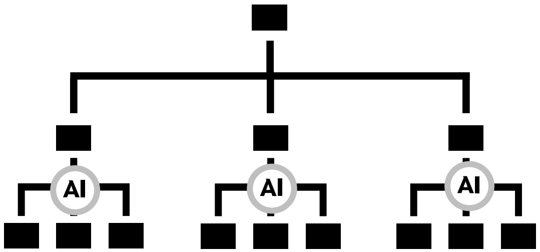
Introduction

NETWORKING

- Machine Learning and Artificial Intelligence is being widely used in a variety of applications
- However, not much used for the networks itself
- When used, build around dedicated, closed and proprietary solutions
- Open interfaces and smart feature extraction will enable and boost the usage AI/ML for Networking
- Disaggregation: Mix & match Networking gear with AI/ML solution

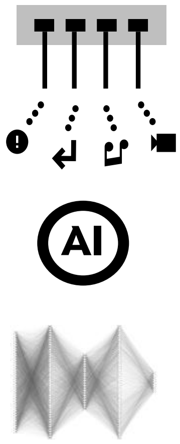
Agenda

- Use cases of AI/ML for networking
- Tools for AI/ML for Networking
- The role of OCP in AI for Networking
- Example Use Case: High-rate anomaly detection



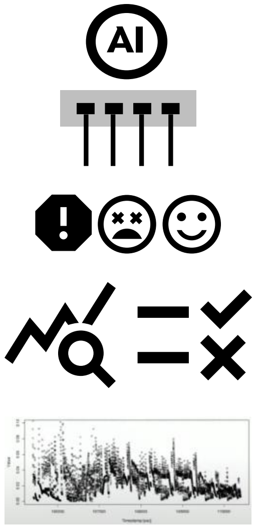
AI/ML for application classification

- Classify Flows to applications
- Handle encrypted packets including encrypted headers
- Assign Class of Service profiles to classified flows
- Assign ACL rules for different applications
- Mostly based on Supervised learning (tagged data)



AI/ML for anomaly detection

- Identify anomalous behavior in the network:
  - Malicious flows
  - Denial-of-service attack
  - Faults of devices
  - Misconfiguration causing abnormal behavior
  - Content theft
- Could be based on supervised and unsupervised learning (tagged and non-tagged data)



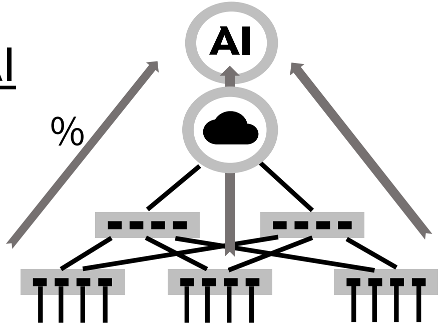
AI/ML for automated networks

- Analyzing complex and large log files
- Correlating events for identifying network faults and configuration errors
- Network Planning and configuring complex networks
- Device identification based on traffic behavior

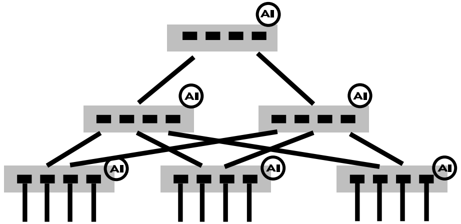
Tools for AI/ML for networking

- Centralized AI/ML – Sharing resources and serving many networking devices
- Distributed AI/ML – Closer to the source of data
- Need continuous and live AI/ML monitoring of network behaviors

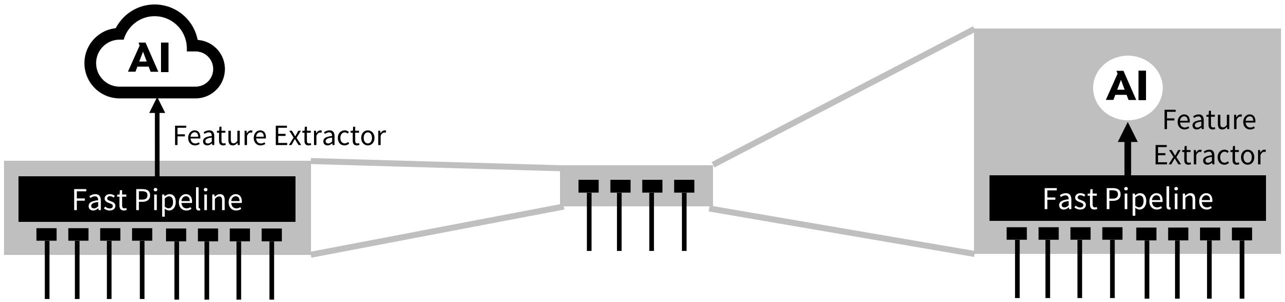
Centralized AI



Distributed AI



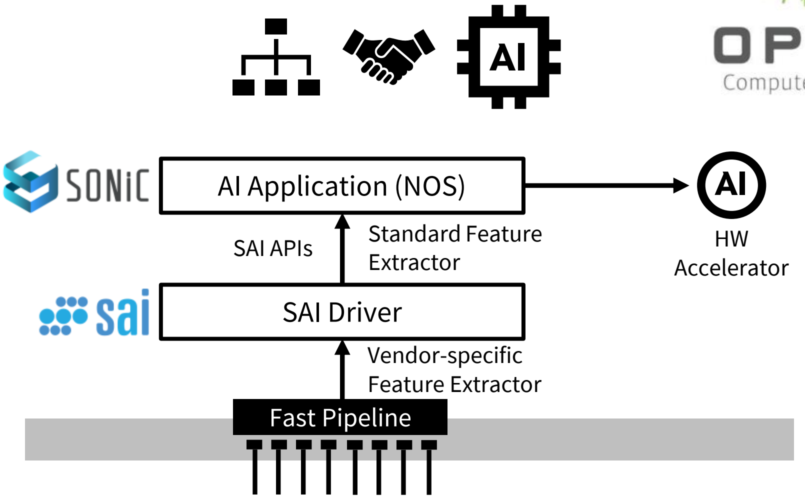
Smart continuous feature extraction



- Condensed telemetry / smart feature extraction is needed for both remote and local AI Engines
- Smart feature extraction enabled continuous traffic inference
- AI Operations per second << Network's packets per second

The role of OCP in AI/ML for networking

- SAI TAM (Telemetry and Monitoring) interface between Switch device and a CPU/AI engine
  - Enhance SAI TAM 2.0 to address AI Use cases
  - Data Formats – Optimized / compressed data structure
  - Scheduling – Trigger for data transfer
- SONIC AI Application – Build AI application as part of Sonic



OPEN Compute Project

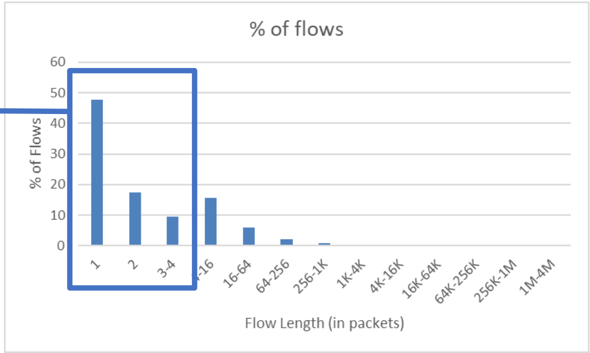
OPEN POSSIBILITIES.

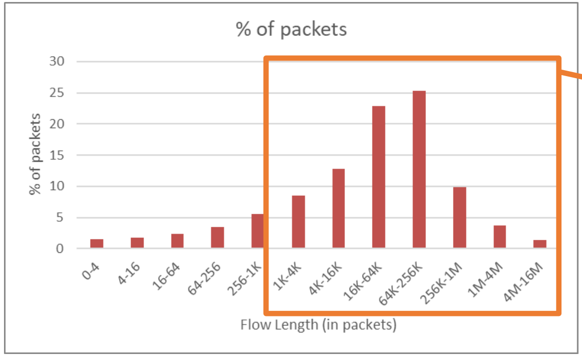
MARVELL

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Data reduction techniques – Beginning of flow

75% of flows are 4 packets or smaller





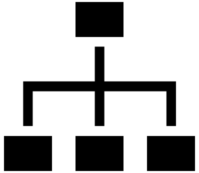
85% of Packets are from flows larger than 1000 packets

Source: "Flow length and size distributions in campus Internet traffic" by Jurkiewicz et al.

- The average flow size is 78 packets
- Analyzing only the first N packets of all flows, reduces the amount of monitored traffic to ~5% when N=4
- Filtering away 1-2 packet flows (like DNS packets), reduces the amount of monitored flows and rate of new flows

Data reduction techniques – Traffic signature

- Continuous queue or flow behavior monitoring
- Benign flows can turn into malicious flows, thus continuous monitoring is needed
- Flow Signature is created by smart statistics based on Packet sizes and packet arrival time – Providing a compressed representation on the traffic patterns



Open AI/ML models for networking

- IOT Device Signature – ONNX Models for device identification and normal behavior
- Flow classifications – Signatures of benign and malicious flows
- Networking Logs – Agreed Data structures to be processed by AI machines corelating events and replacing humans in reaching conclusions

OPEN POSSIBILITIES.

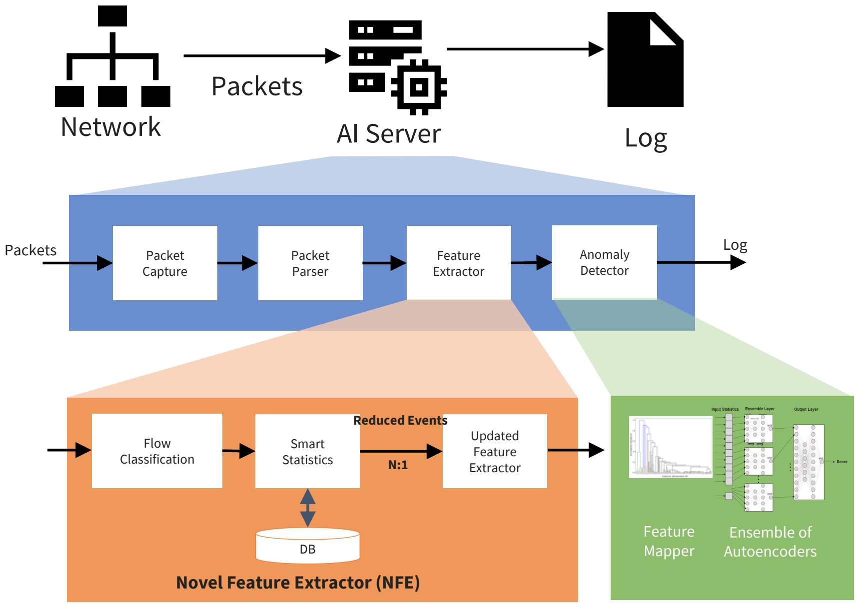
Example Use Case:

High-rate anomaly detection in Networking

OCP GLOBAL SUMMIT

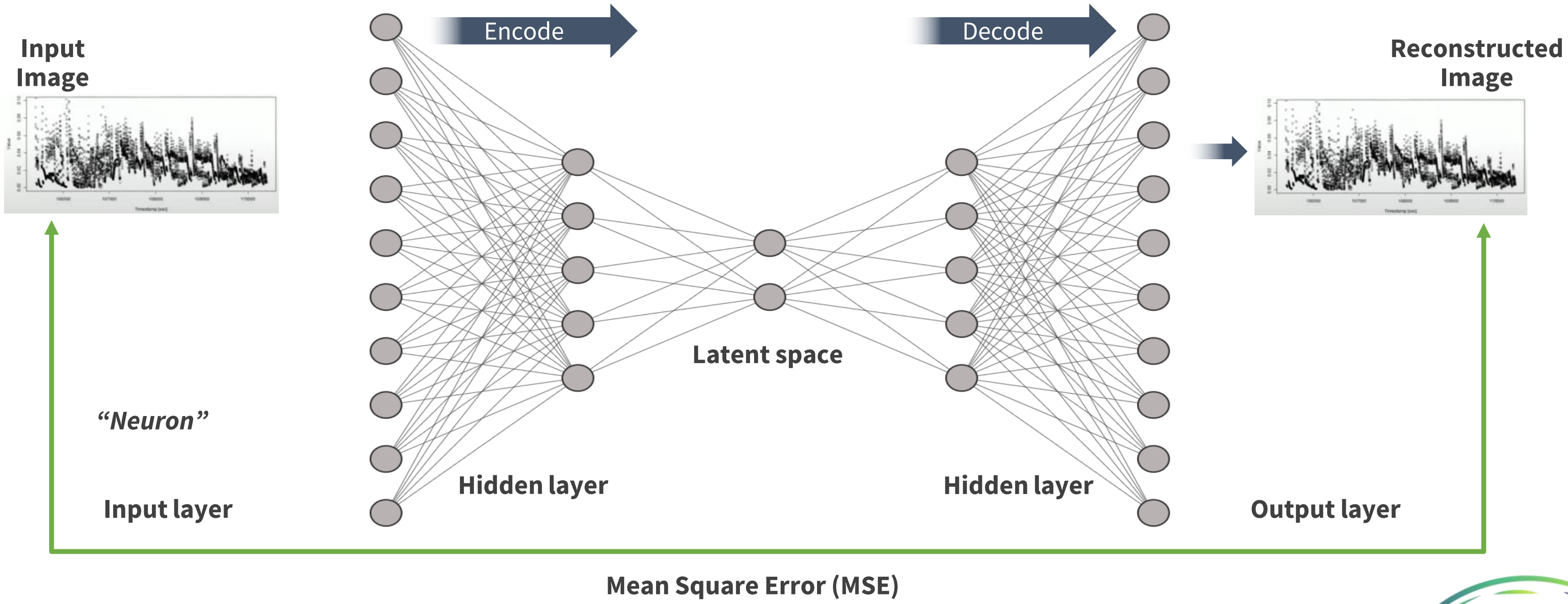
NOVEMBER 9-10, 2021

Anomaly Detection Framework



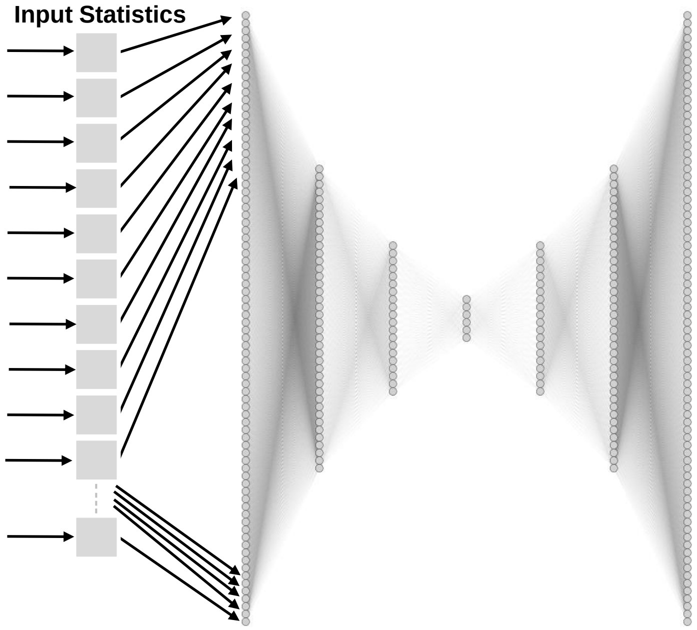
- A feature extractor with reduced number of events per sec
- Provides smart statistics on group of packets instead of a by-packet basis
- ‘Signatures’ instead of ‘raw data’
- Damped incremental statistics with Multiple decay factors
- Ensemble of small neural networks (auto encoders)

Autoencoder Model Architecture

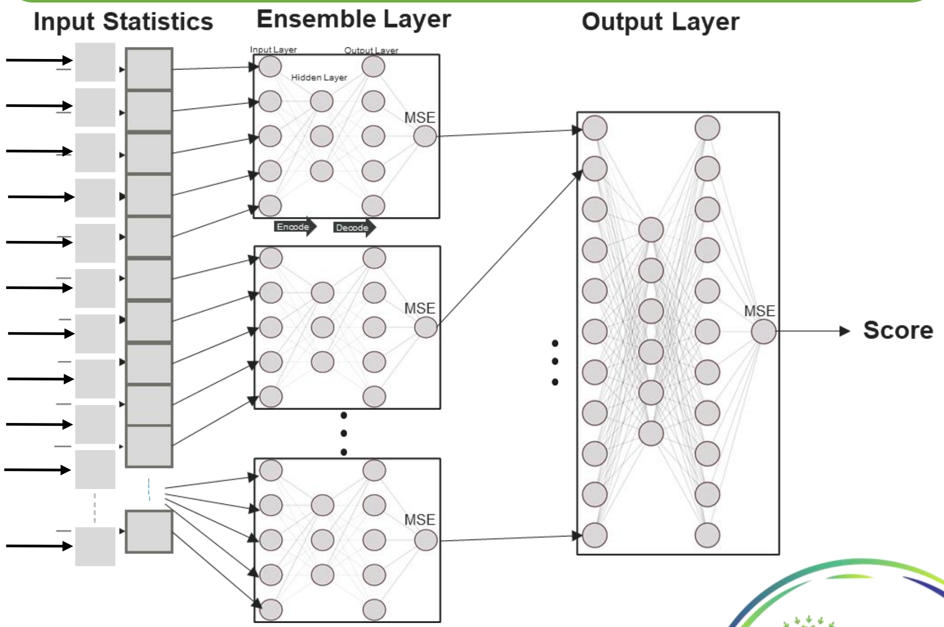


Ensemble of Auto Encoders

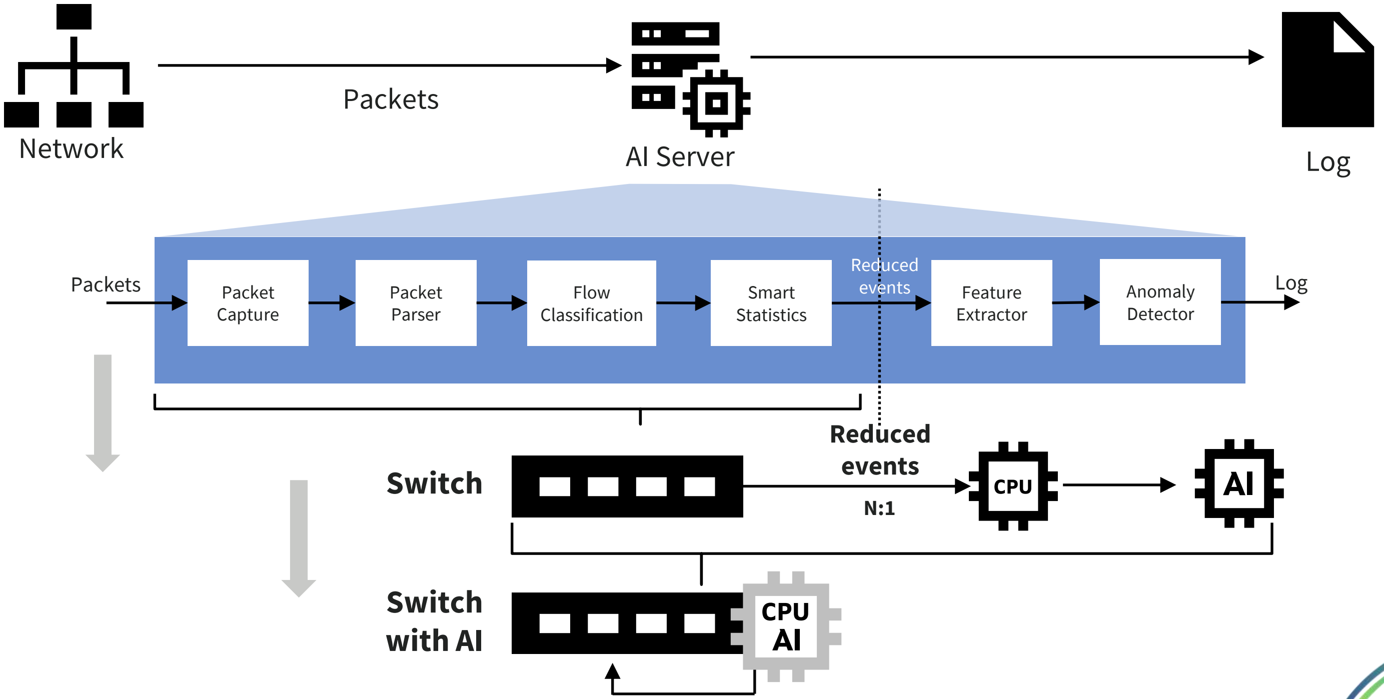
One neural network



Ensemble of neural networks

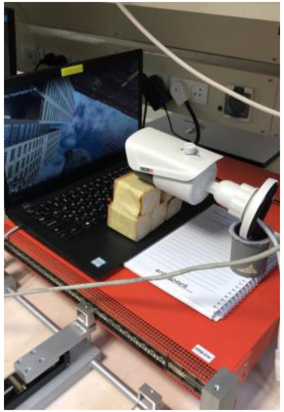


Enhanced framework



Test Bed

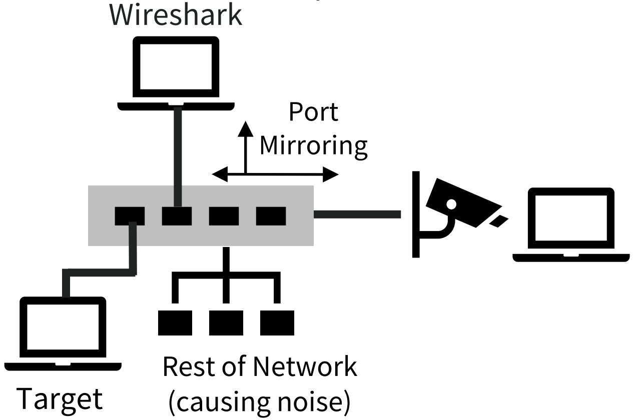
Identifying anomalies in sensor behavior



Training phase was done on running normal traffic

Inference phase

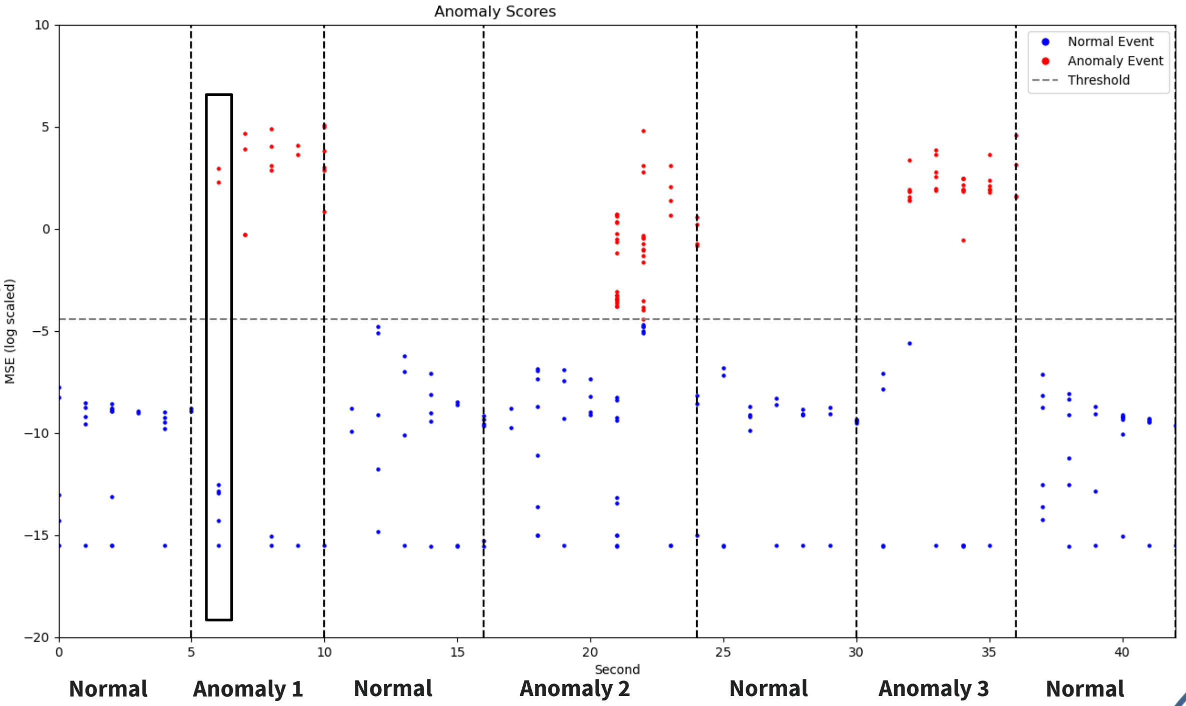
- Normal
- Anomaly 1 – Different Camera setup
- Anomaly 2 – Traffic sent towards the camera
- Anomaly 3 – Potential unauthorized clients consuming traffic



Anomaly Detection – Test Bed Results

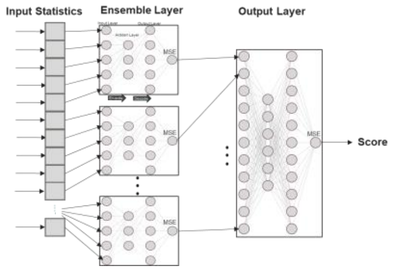
Anomalies
Reconstruction loss (MSE) > Threshold.

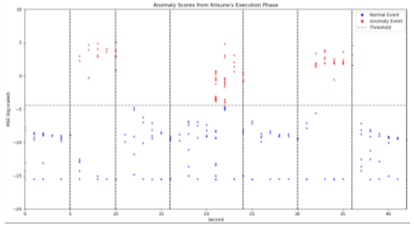
Normal
Reconstruction loss (MSE) < Threshold.



Summary

1. AI/ML for networking has many exciting use cases, such as anomaly detection
2. OCP to define open interfaces between networking devices and AI engines
3. Networking devices to provide smart reduced statistics/telemetry for AI processing
4. Accurate and high-performance anomaly detection is possible in high-speed networks





OPEN POSSIBILITIES.

MARVELL

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

OPEN POSSIBILITIES.

Thank you.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

MARVELL™

Essential technology, done right™