Intrusion Detection Adapted for Automotive – Challenges for Hardware - An Implementation Example

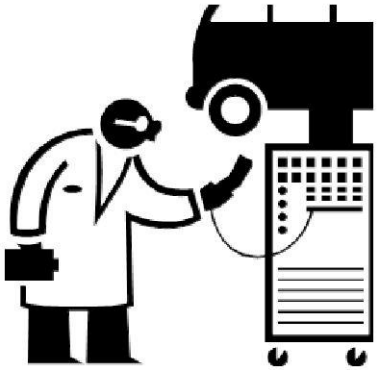
IEEE STANDARDS ASSOCIATION IEEE

2018 IEEE-SA Ethernet & IP @ Automotive Technology Day
Harald Zweck, Infineon Technologies
Ronny Schulze, Infineon Technologies

Infineon

Motivation

Statement given by “I Am The Cavalry”



Evidence Capture

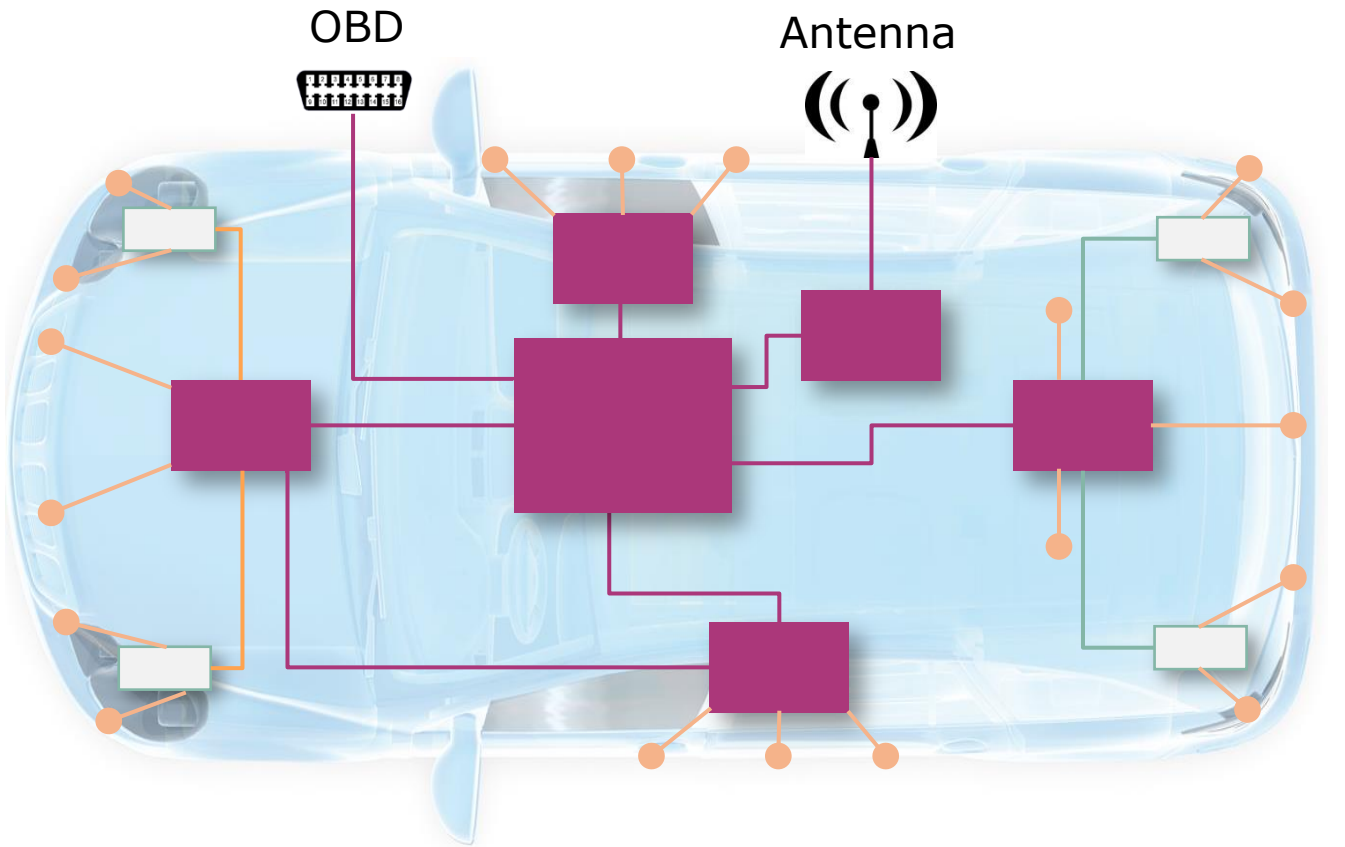
Safety investigations drive substantial improvements, and **records of electronic systems operations give visibility into root causes that may otherwise be opaque. These records can plainly show sources of error, be they malfunctions, design defects, human error or deliberate attack**. Those waiting for proof of hacking or electronic sabotage will not find evidence without such logging and evidence collection in place. This capability will require more effort, over time, than others on this list, but it is foundational for improving safety in the long-term so starting now will help us achieve this goal.

Do your vehicle systems provide tamper evident, forensically-sound logging and evidence capture to facilitate safety investigations?

I read => Electronic systems shall record events like malfunctions, defects, errors, attacks etc.

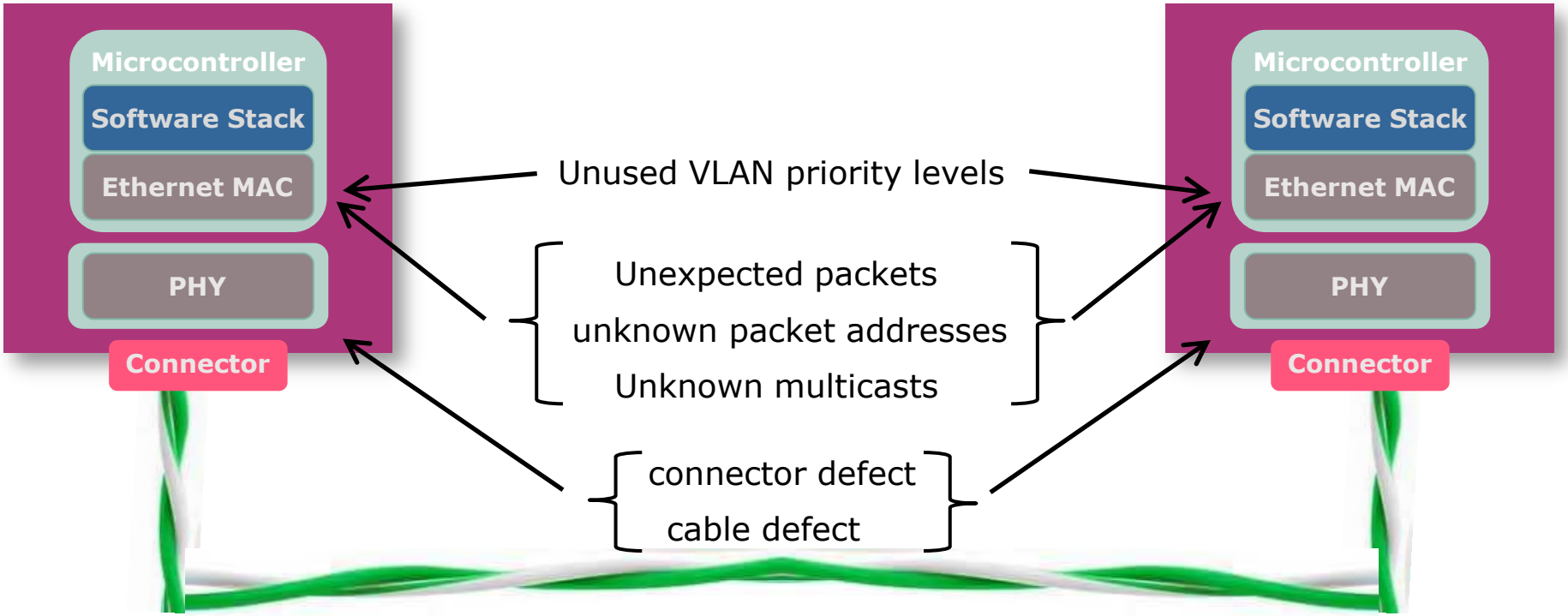
Source: I Am The Cavalry / Five Star Automotive Cyber Safety Framework / February 2015 / Link: https://www.iamthecavalry.org/

Network


OBD
Antenna
Automotive Ethernet
CAN / Sensor Bus
ECU with Ethernet connectivity
ECU

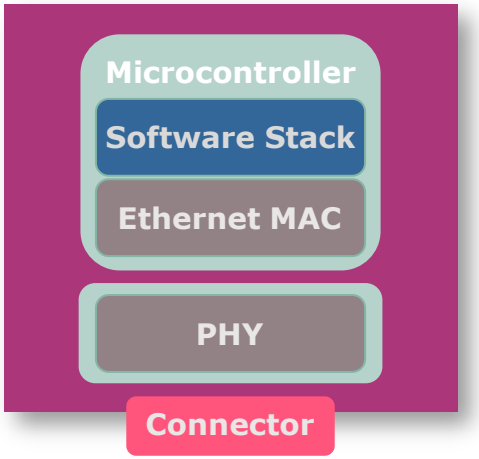
Network Traffic Clustering

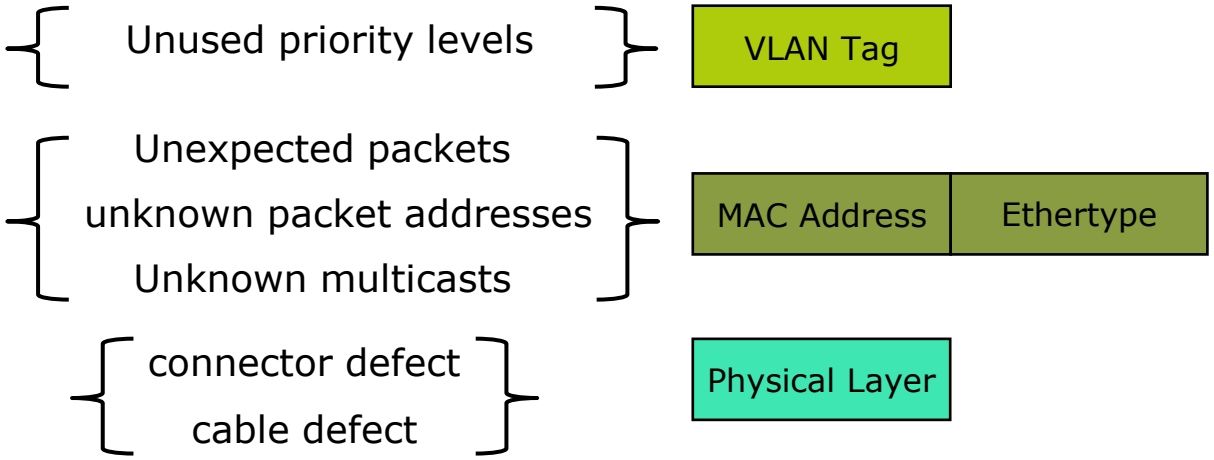
› Unexpected traffic example related to Microcontroller Units



Network Traffic Clustering

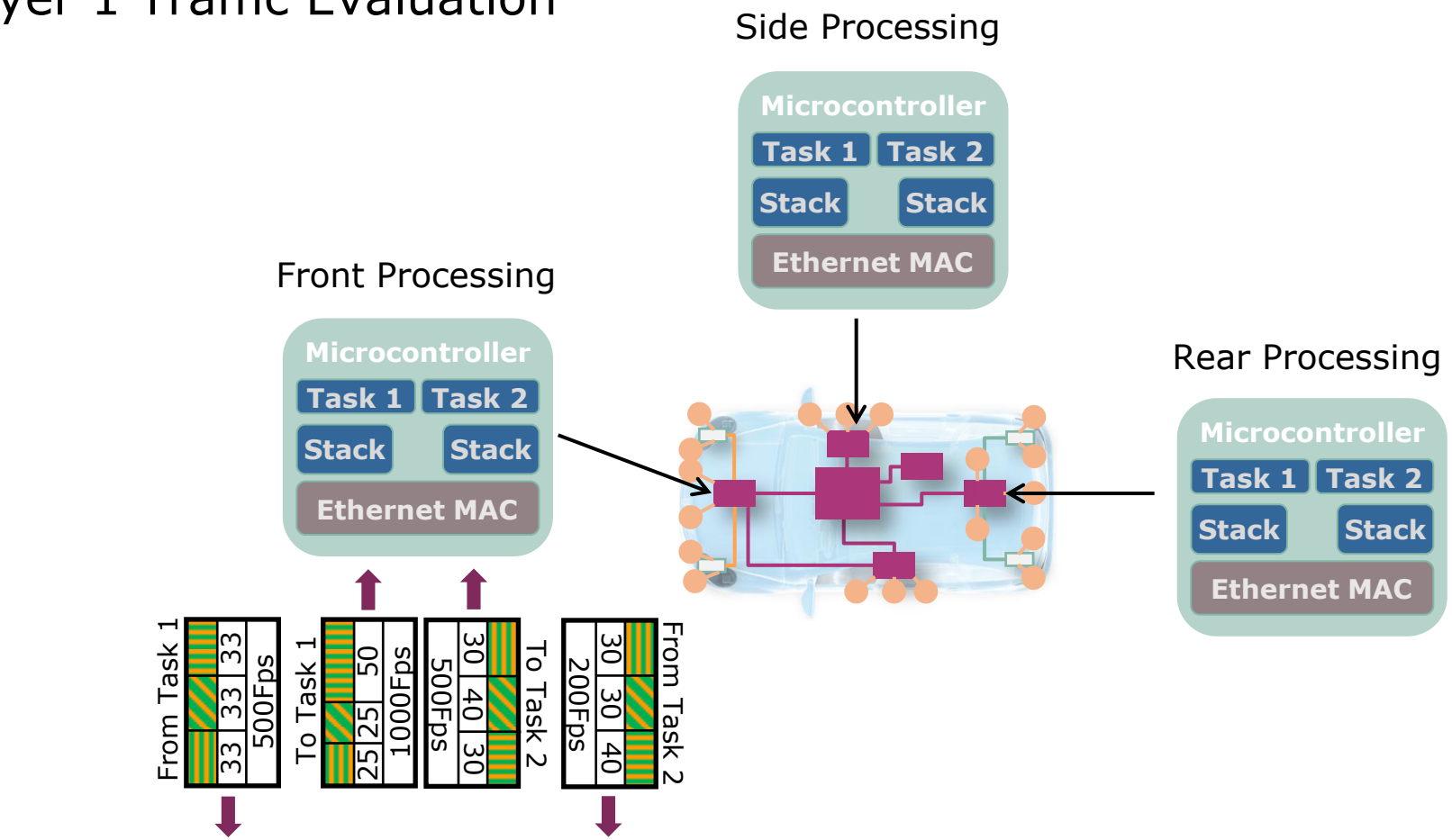
› Unexpected traffic example related to OSI Layer 1 / 2 / 2.5





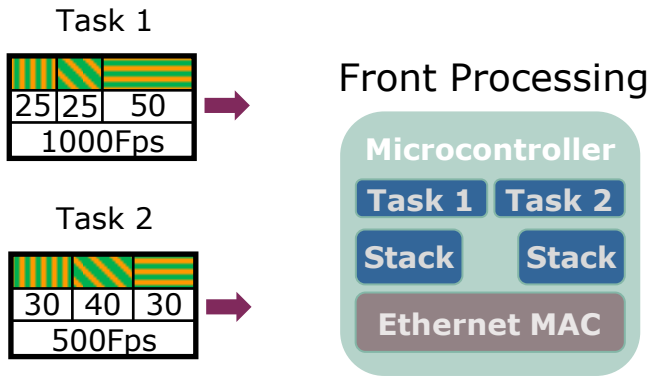
Network Traffic Monitoring – Layer 1

› Layer 1 Traffic Evaluation



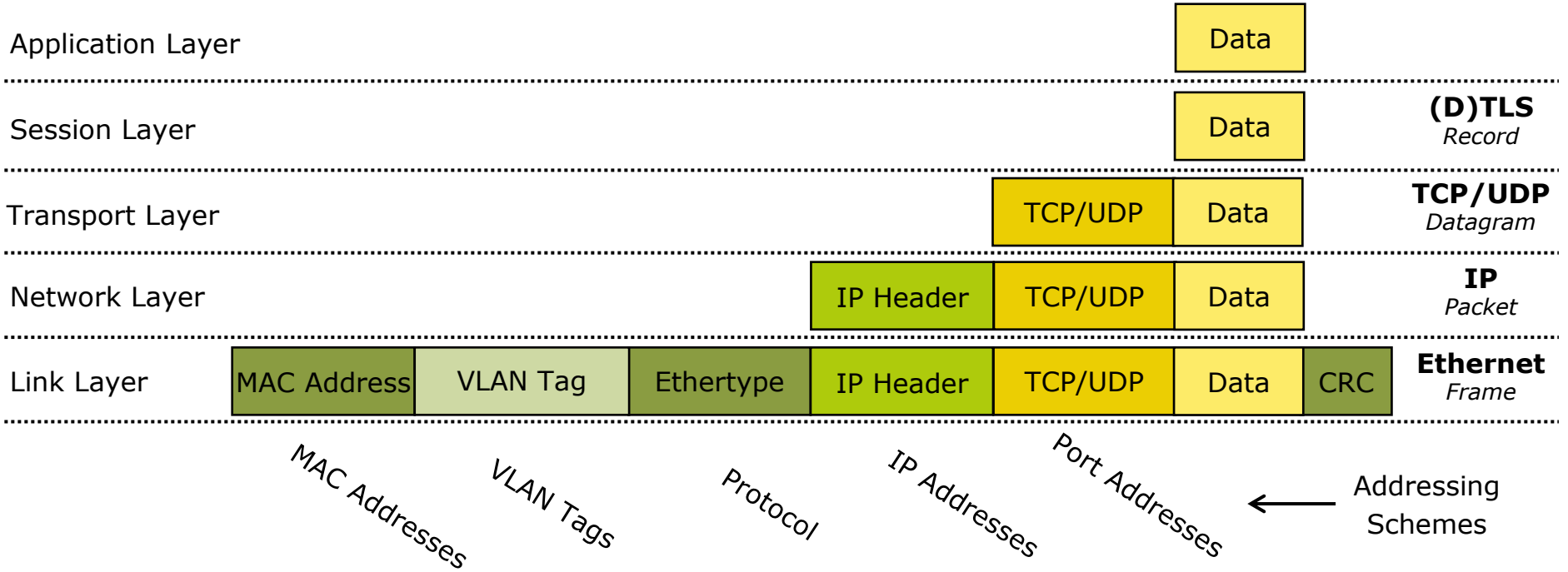
Network Traffic Monitoring – Layer 1

› Layer 1 Traffic Evaluation Example – Based on Frame Length



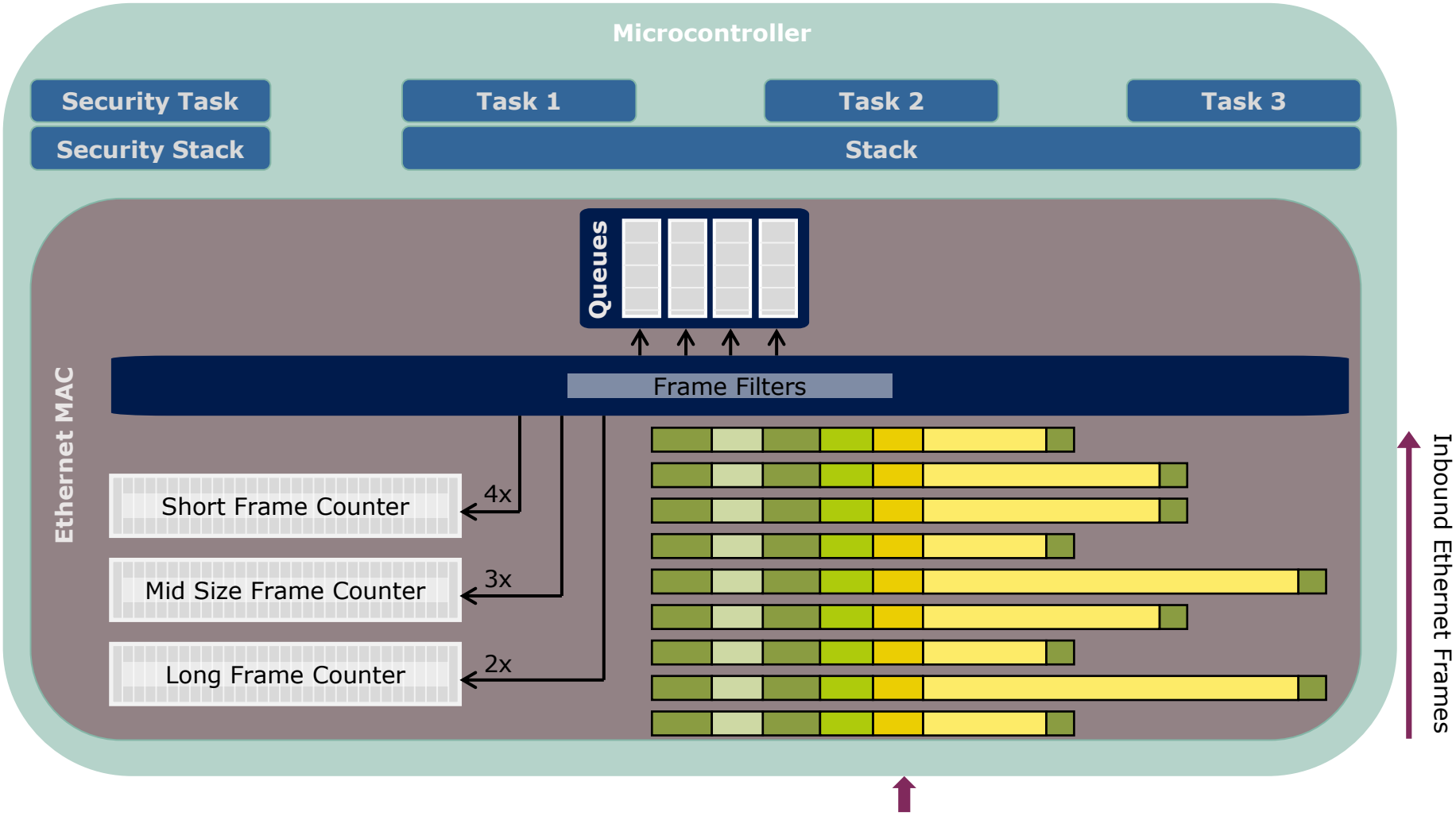
Frame Profile (length in bytes)		Task 1 reception	Task 2 reception	Total
	Short frame < 128	50% of 1000Fps => **500Fps**	30% of 500Fps => **150Fps**	500Fps + 150Fps => **650Fps**
	Mid range frame 128 < frame < 1023	25% of 1000Fps => **250Fps**	40% of 500Fps => **200Fps**	250Fps + 200Fps => **450Fps**
	Long frame > 1023	25% of 1000Fps => **250Fps**	30% of 500Fps => **150Fps**	250Fps + 150Fps => **400Fps**

IEEE Standard Ethernet Frame



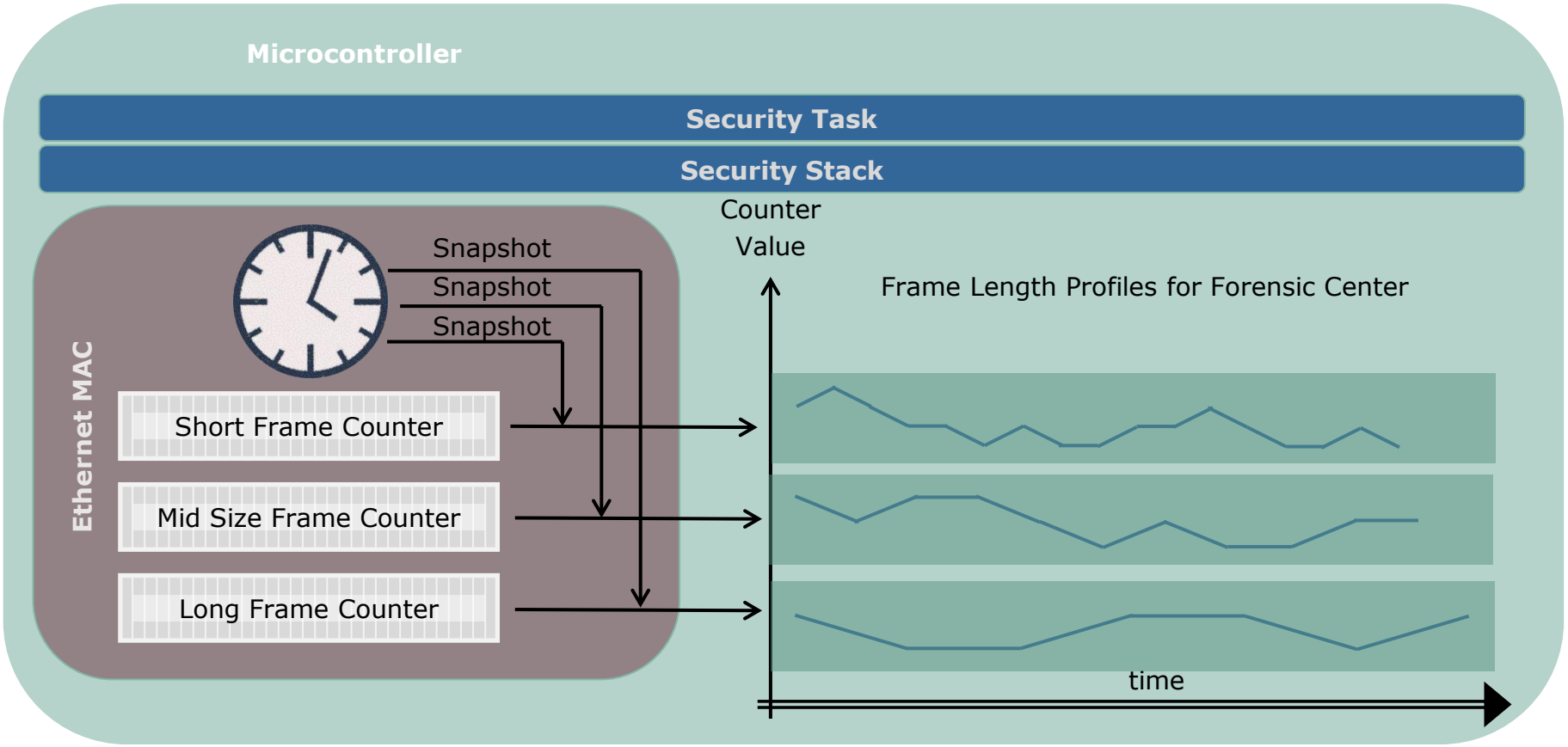
Network Traffic Monitoring – Layer 1

› Layer 1 Traffic Monitoring Example – Based on Frame Length



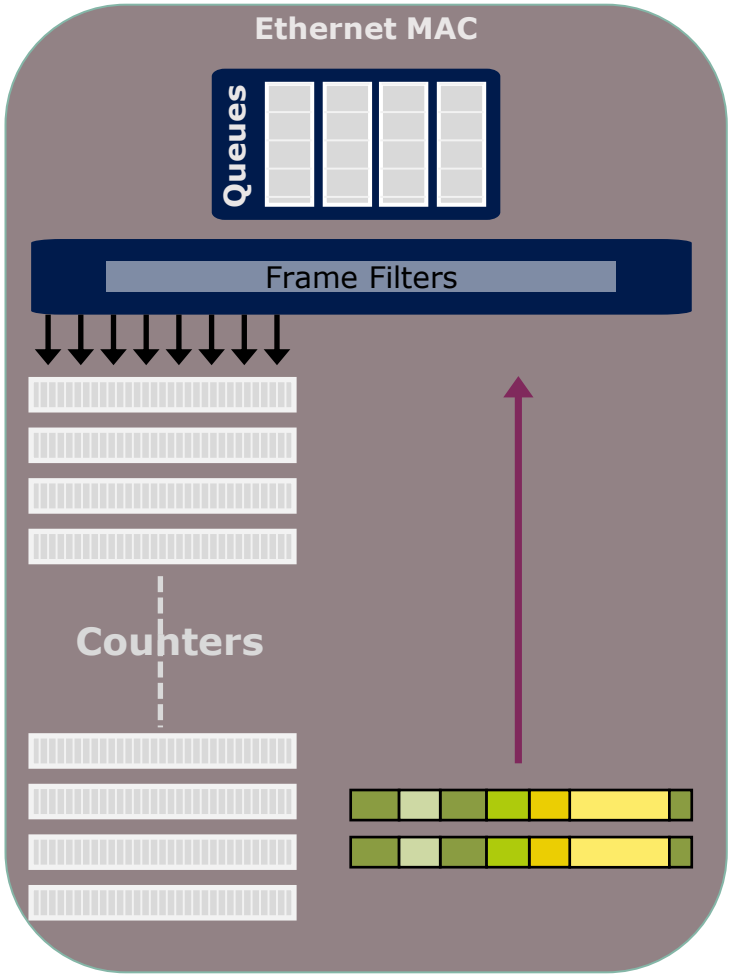
Network Traffic Profiling – Layer 1

› Layer 1 Traffic Profiling Example – Based on Frame Length



Network Traffic Profiling – Layer 1

› Layer 1 - Limitations



Not Covered

- VLAN Tag Priority (PCP) → VLAN Tag
- Packet Addresses → MAC Address

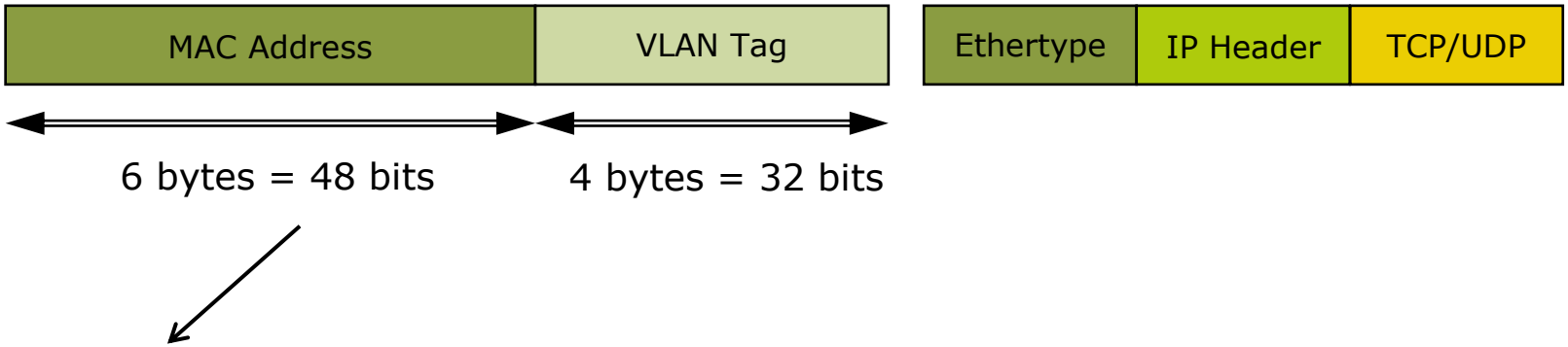
Covered

- Broadcast
- Multicast
- Frame Length
- CRC Error

→ Physical Layer Frame Layer

Network Traffic Profiling – Layer 2

- Layer 2 - Challenges

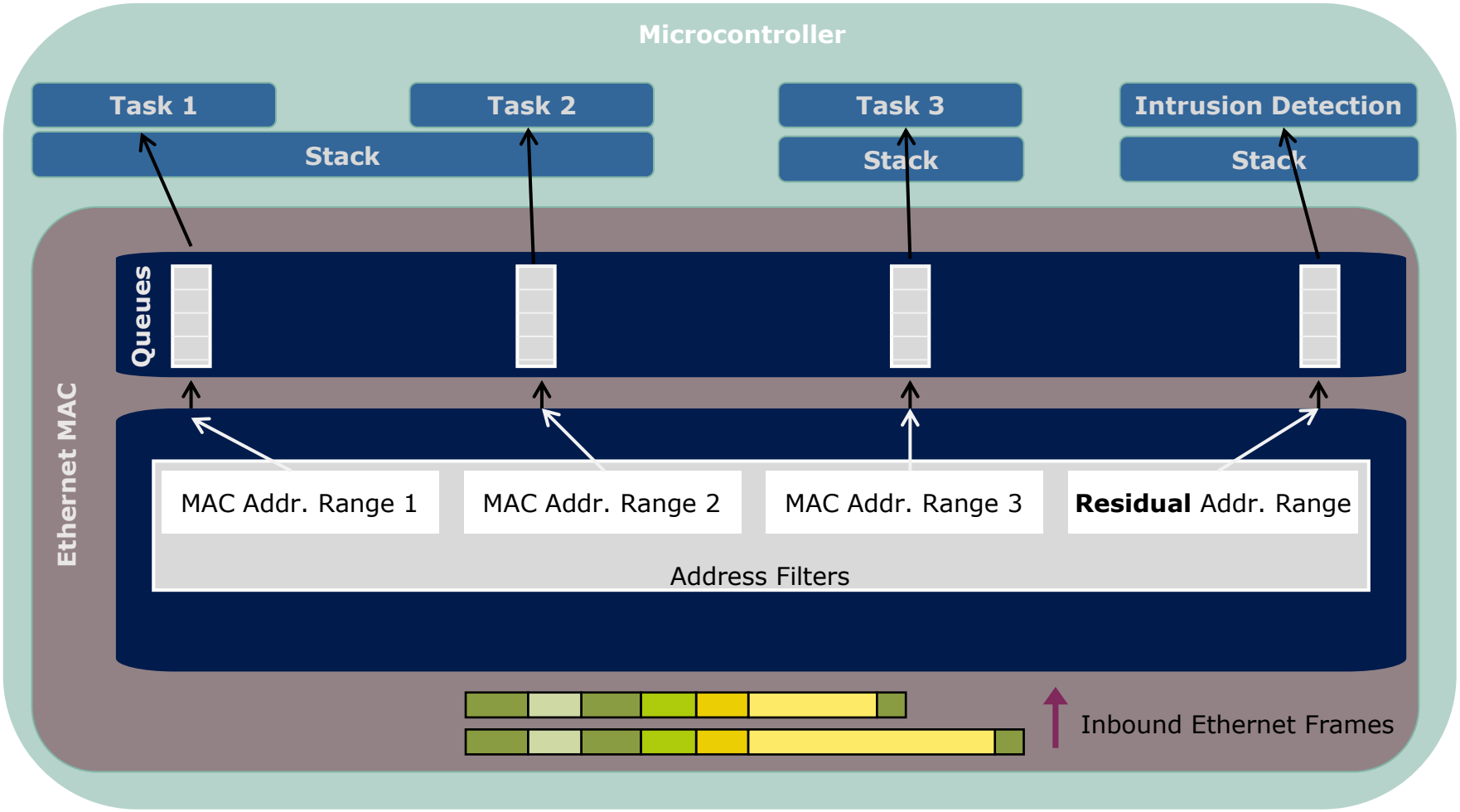


- 2^{48} counters ??

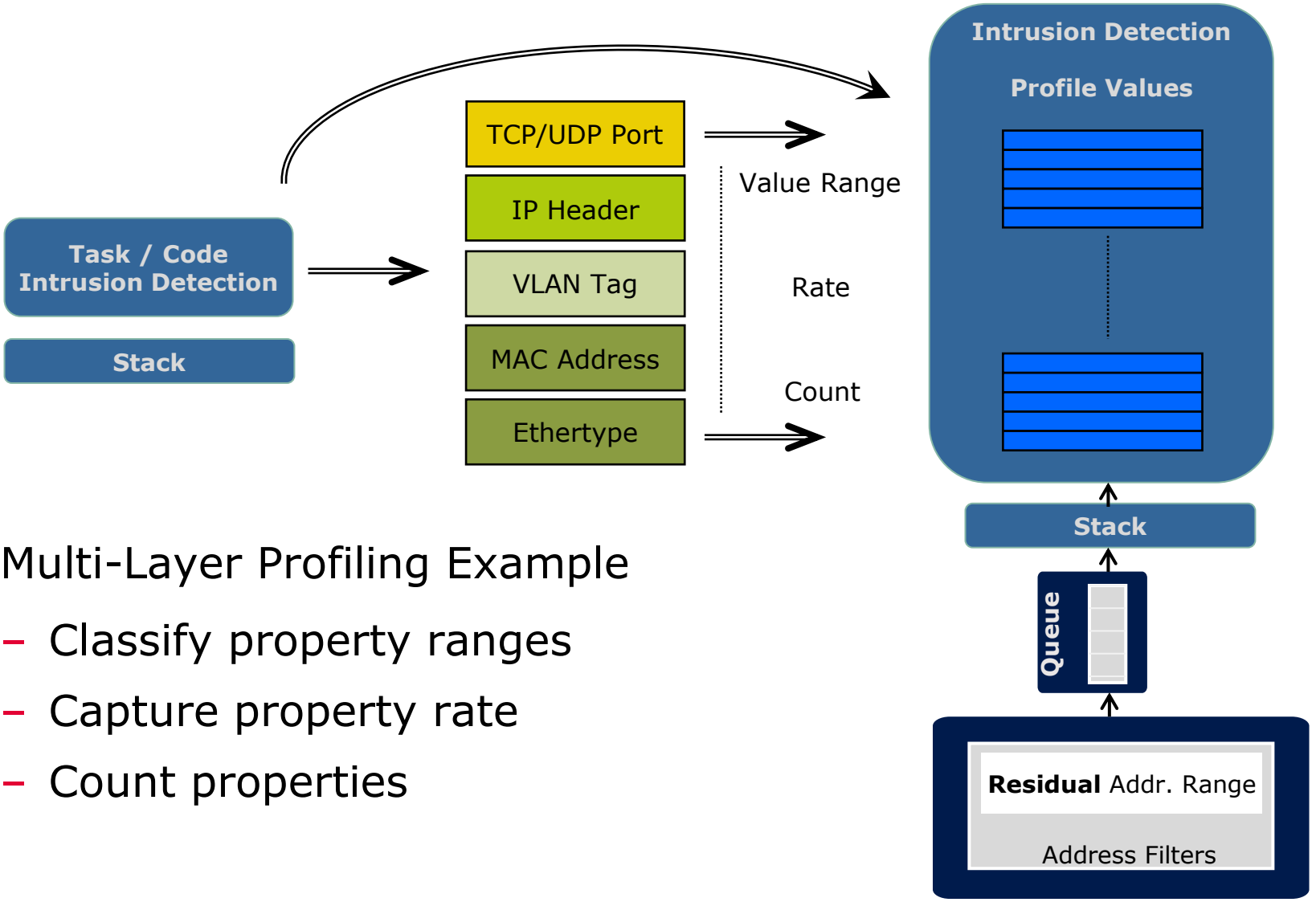
- Realistic solution:
  - Capture counters for passing frames -> 2 digit number range
  - Capture rejected frames in one special stack process

Network Traffic Profiling – Layer 2

› Layer 2 Ethernet Frame Profiling



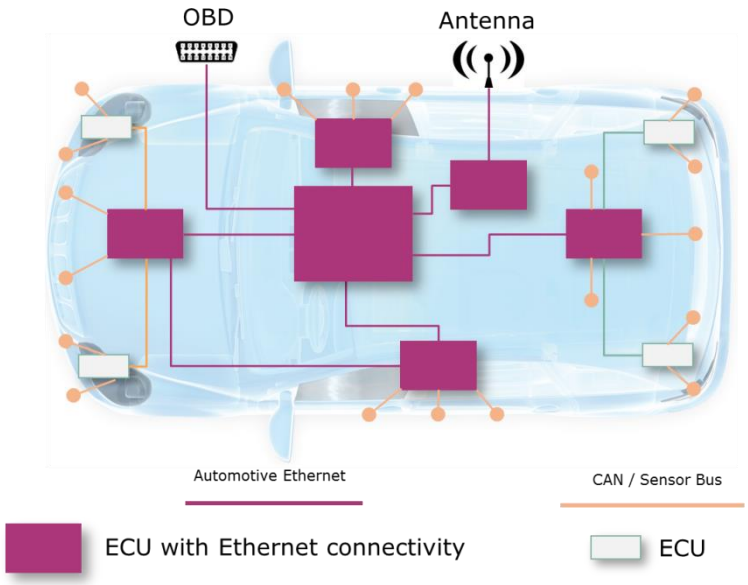
Network Traffic Profiling – Layer 2



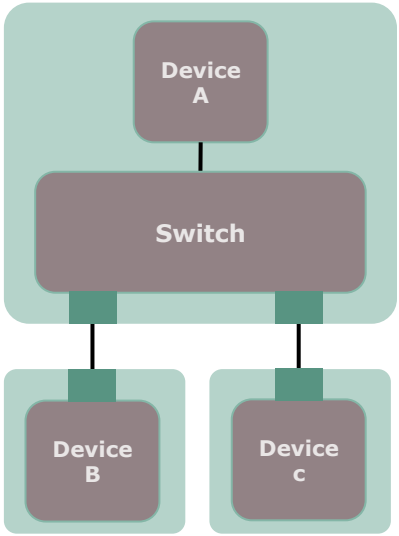
- Multi-Layer Profiling Example
  - Classify property ranges
  - Capture property rate
  - Count properties

Simplified Network Demo

- Switched networks – Expectations
  - Intelligent packet routing by switches
  - Switches provide as well features for traffic analyzes

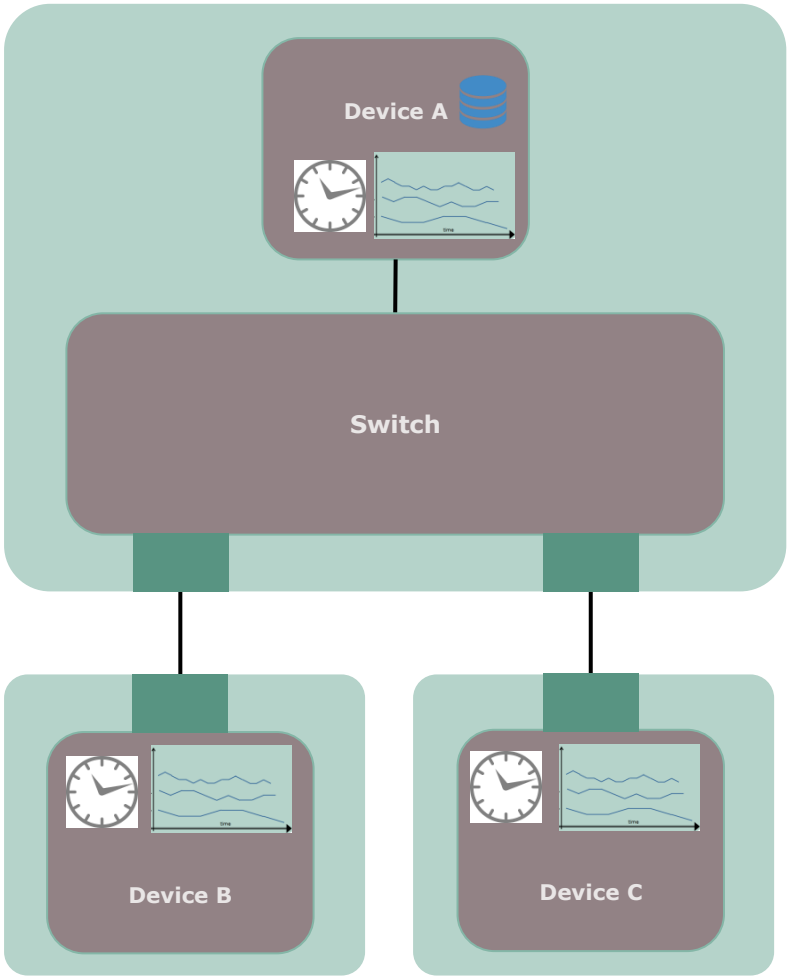


Demo Network



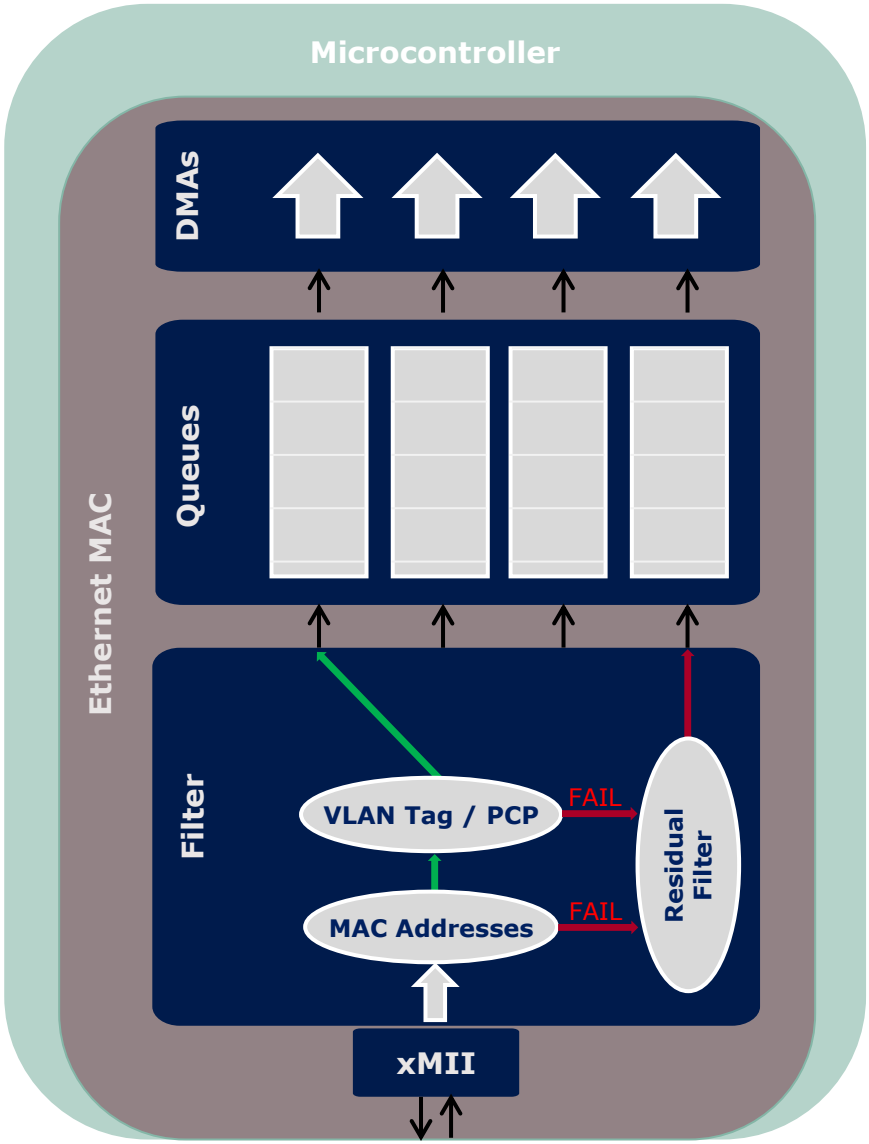
Traffic profiling/monitoring

- Using Hardware support in form of IETF MIB counter inside the Ethernet MAC
  - Using register for number of good and bad packets with different length
  - We count frames with a length of 64to 256 bytes, 256 – 512 bytes and 512 to 1023 bytes
- Device B and C will send there profile in a cyclic way to device A



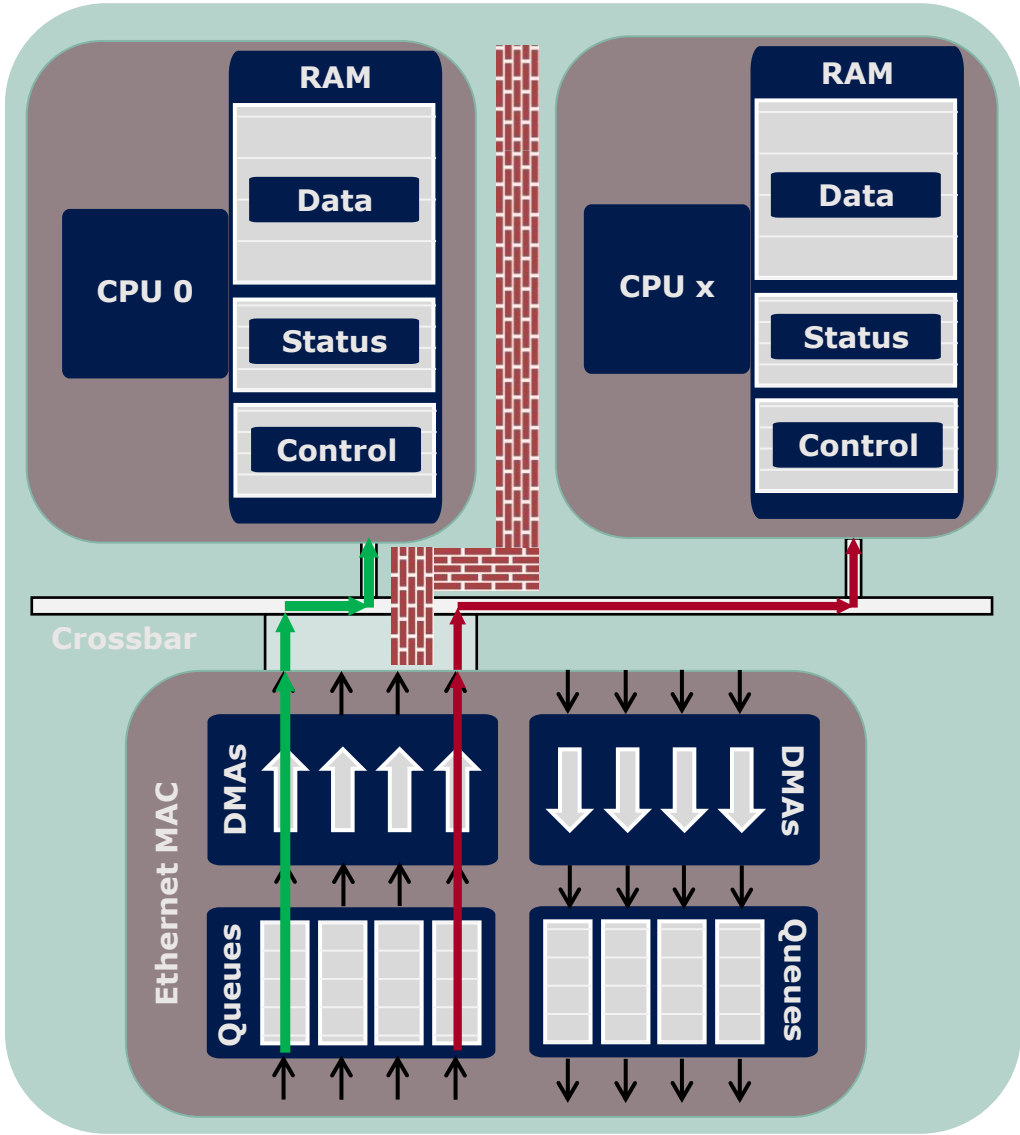
Layer 2 implementation of residual Filter

- Packets which not pass the Uni/multicast addresses or VLAN filter will **not** be dropped
- These packets are forwarded to a residual filter queue
- Separating these traffic allows to route the traffic to a independent CPU inside the MCU to analyze



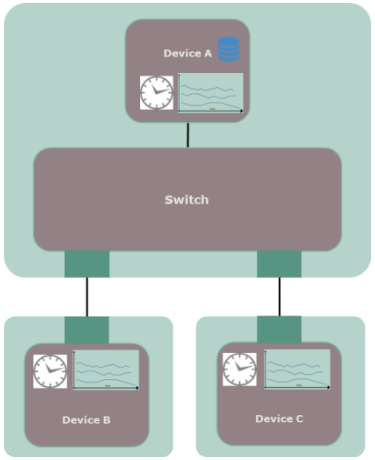
Separating traffics inside the MCU

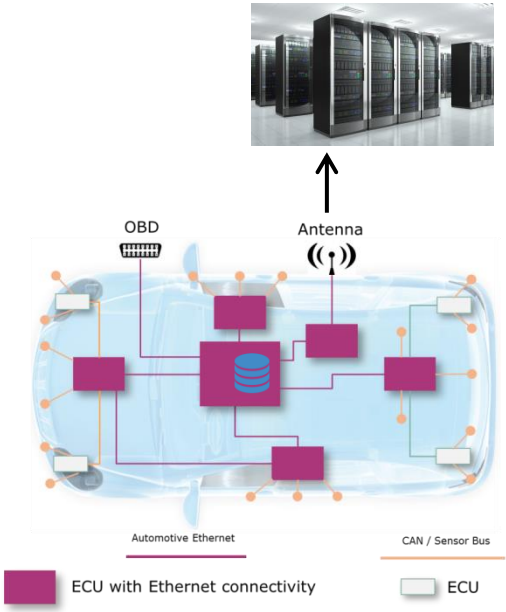
- Sorted packets inside the residual queue can be forwarded to an separate/isolated CPU to process the data independent
- CPU x counts periodical packets based on MAC addresses, Types etc…



At the End …

- What to do with all that data?
  - Device B and C will report their traffic behavior to Device A which manage the switch
  - Device A can analyze and may change the configuration of the switch ports for Device B and C
  - Device A sends the network healthiness state to a forensic center





- *See the Demo at the Infineon booth!*

Part of your life. Part of tomorrow.