

Maxeler Apps

Line Rate Packet Capture



Dec 2014

Line Rate Packet Capture

Problem

With the speed and bandwidth of networks increasing as more services are transitioning online it becomes highly important to understand what data is being transferred across a network.

Current packet capture solutions are lossy and tend to make sacrifices on what data is logged due to these increasing demands by:

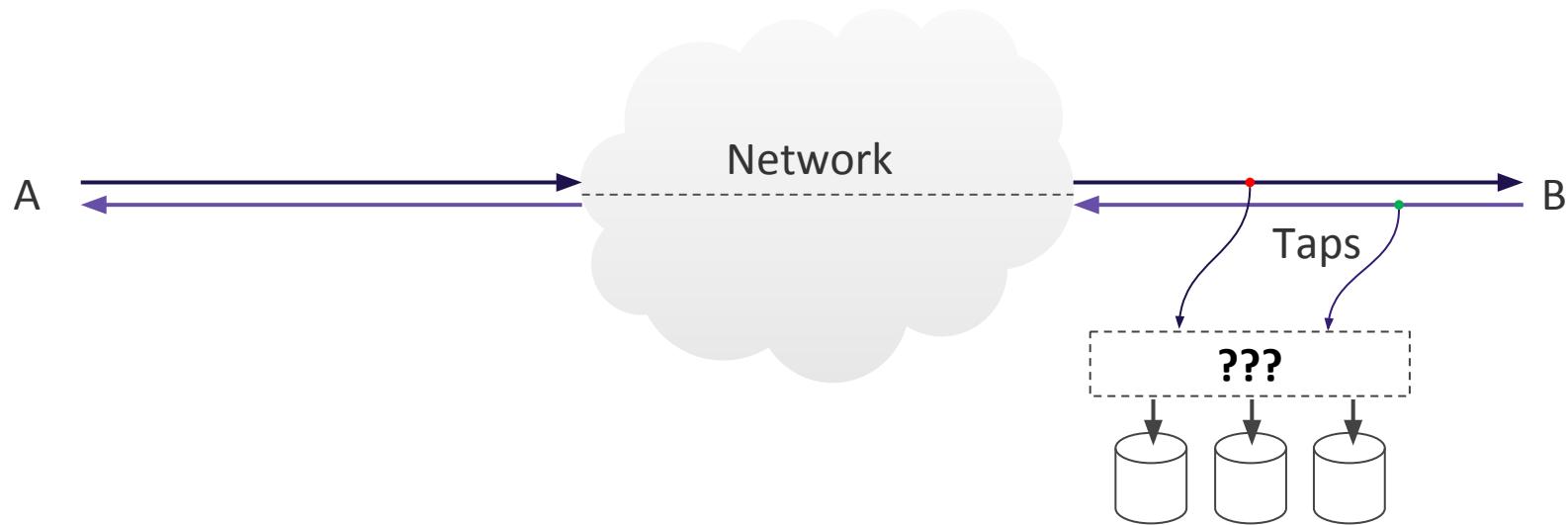
- Filtering traffic on a pre-set criteria
- Sampling a subset of data
- Putting short limits on retention

Existing Software Solutions: Wireshark, tcpdump, pcap, ...

Line Rate Packet Capture

Logging **all** data allows

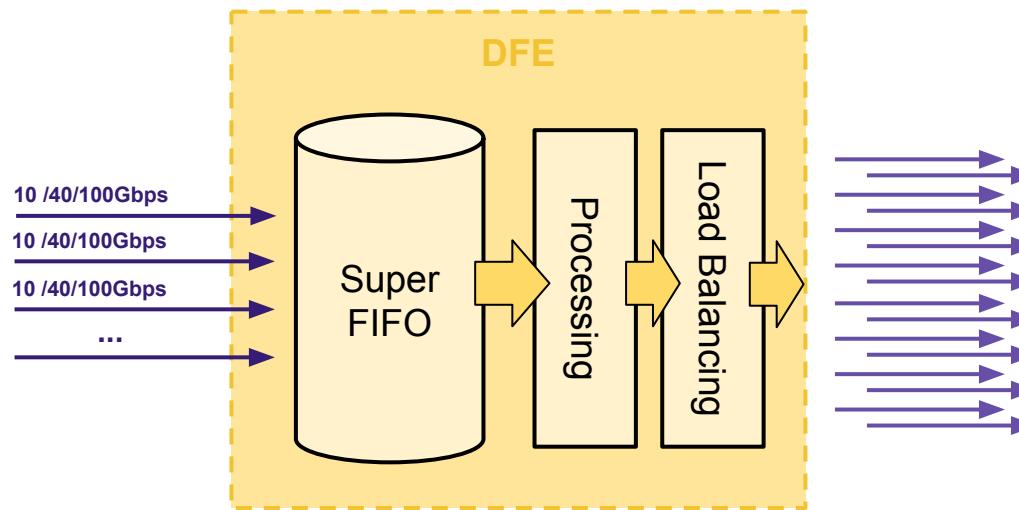
- Retroactive problem solving
- Logging/protecting against cyber threats
- Policy enforcement
- Debugging protocols/services
- Understanding how users use your network



Line Rate Packet Capture

Solution Overview

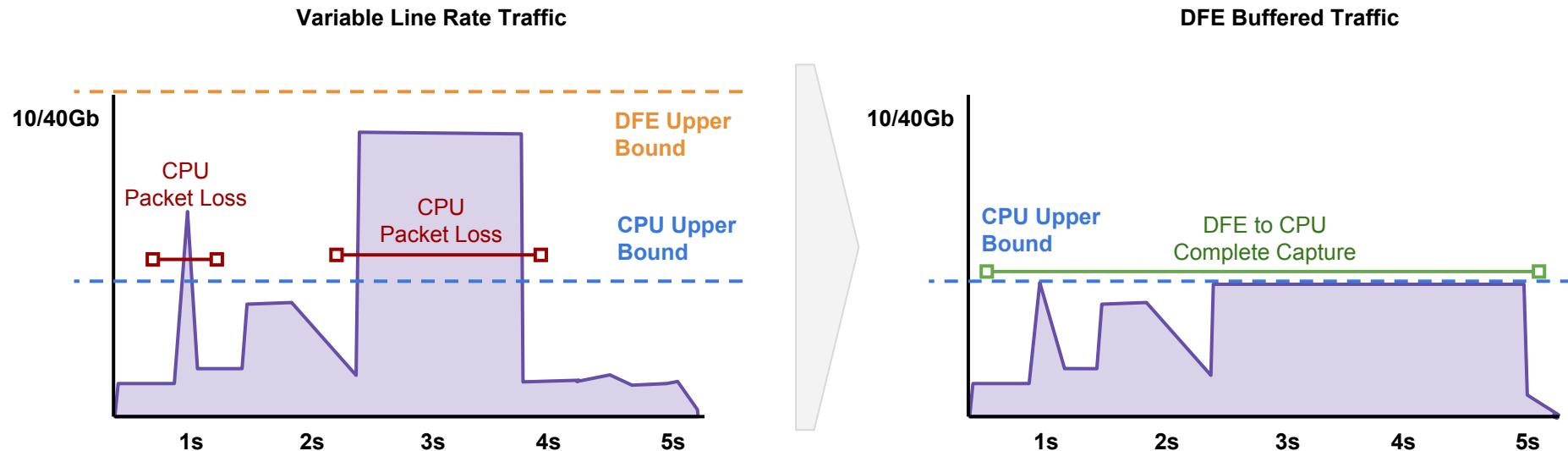
Use a DFE to buffer **all** network data at line rate, process, and pass off to CPU or cluster of storage backends



Use Case: Debugging Protocols

Using a single CPU

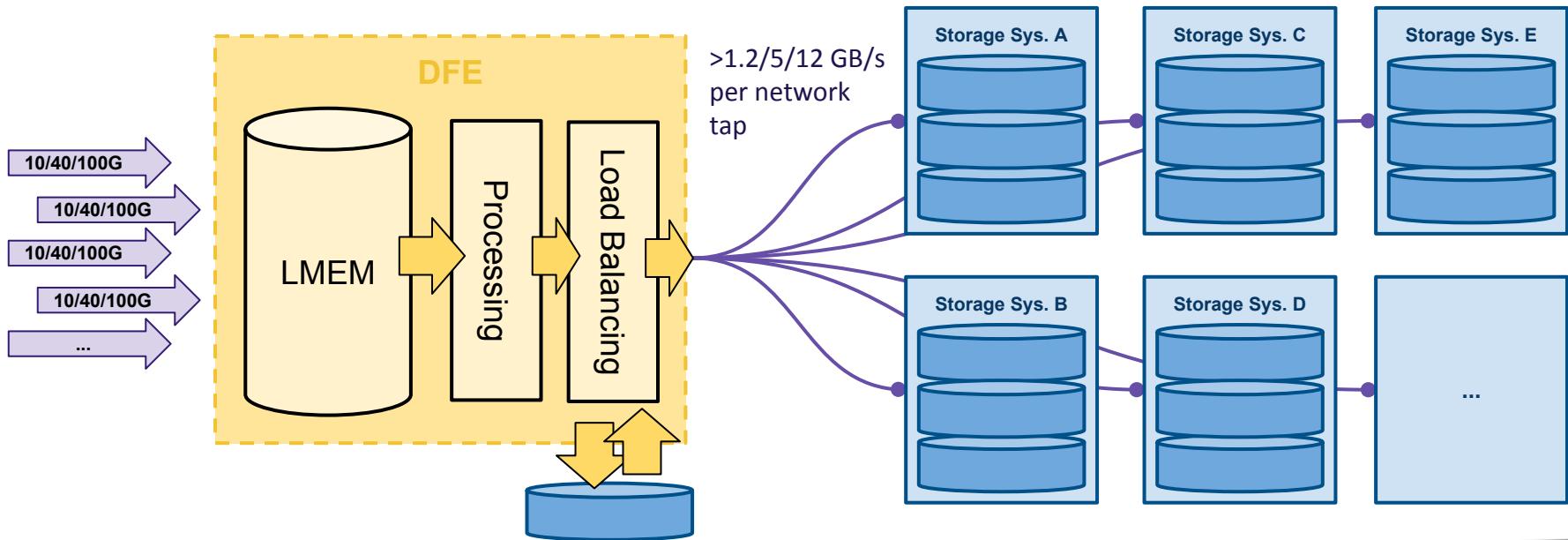
For debugging high speed network protocols it can be impractical or impossible to capture network traffic at line rate. With a single CPU transferring data from a DFE raw network traffic can be captured without packet loss (bursts of up to 192Gb in size, ~5s of full 40Gbps, ~20s of full 10Gbps).



Use Case: Complete Data Retention

Lossless packet capture with storage arrays

For long term data retention the DFE can provide lossless packet capture using dynamic distribution to storage clusters without exceeding maximum throughput for any one array. In the event of short-term unavailability the DFE can buffer to disk and recover.



Use Case: Complete Data Retention

Storage System Requirements

Network Speed	Capture Period [24H]	Required Storage Size [TB]	Required Storage Throughput [GB/s]
10G	1	108	1.25
10G	30	3240	1.25
40G	1	432	5
40G	30	12960	5
100G	1	1080	12.5
100G	30	32400	12.5

For Example: With 8x 40G capture channels the DFE divides full line-rate data between 4 or more high end storage systems (Raid-5, 256 KiB transfers)

Use Case: Recording Packet Ordering

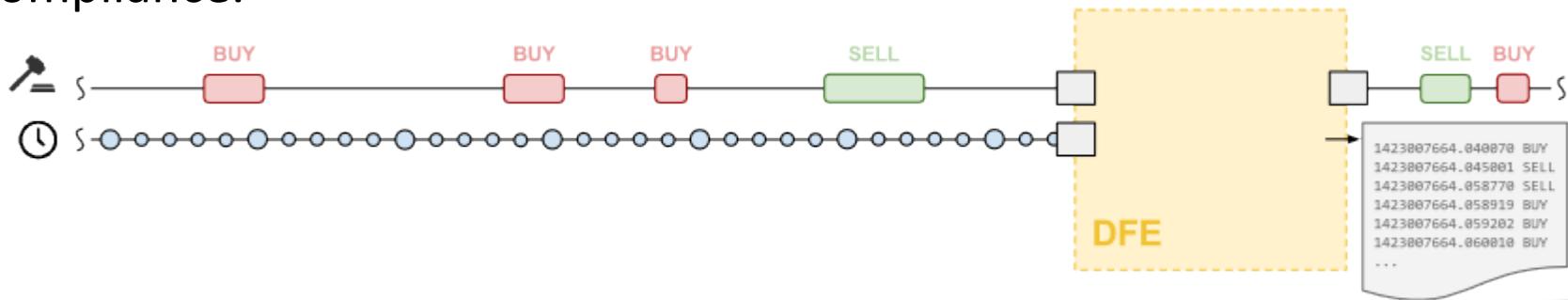
Generate timestamped records of packets at line-rate

For EU Financial Markets the MiFID2 regulations require...

"An investment firm that engages in a high-frequency algorithmic trading technique shall store... time sequenced records of all its placed orders..."

Directive 2014/65/EU of the European Parliament And of the Council Article 17,
2

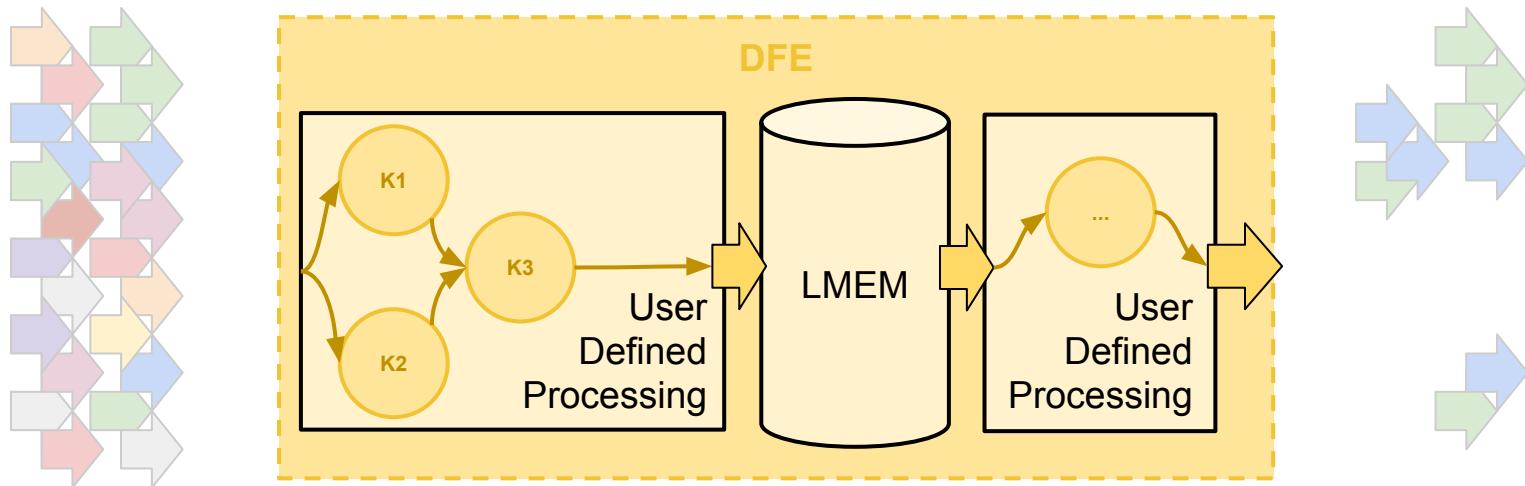
The DFE can be configured to analyze packet data at line rate and record a high precision log of these events to enable regulatory compliance.



Use Case: Line Rate Packet Filtering

Starting point for packet filtering

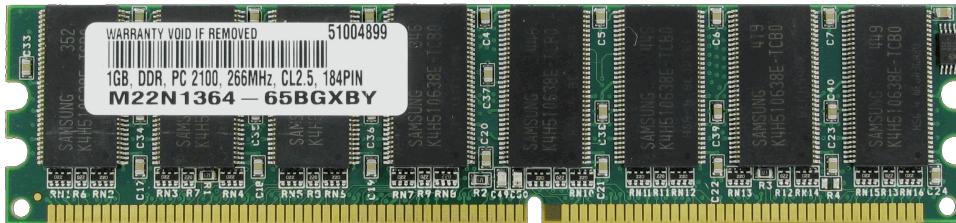
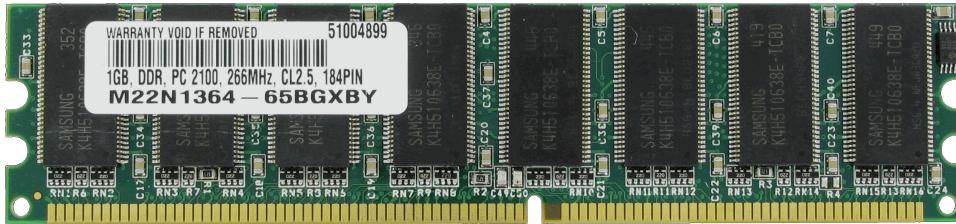
The sample Packet Capture App provides a convenient starting point for a line rate packet filtering application. A user simply needs to add their own processing logic for header inspection and/or deep packet inspection. The MaxCompiler provides APIs to facilitate working with variable length ethernet frames.



Use Case: Demonstrate LMEM

Example of LMEM capabilities

The SuperFIFO implementation is backed by LMEM and is a good example of how large on chip memory can be utilized in a DFE application.



Advanced Impl.

- High-Precision Timestamps
- Filtering
- Decoding
- Compression
- User Defined Behavior
- Stream to Storage System
- Lossless Packet Capture

