

Kill Switch: Hardware-Based Line-Rate Filtering and Capture of 10Gb/s Ethernet Network

CSEE 4840 SPRING 2013 PROJECT PROPOSAL

Working-REAL group:

Qiushi Dingqd2119, Bokai Chenbc2526, Yuyang Wang yw2507,

LihengWang lw2496, Jingshu Fang jf2781

I. Object description

The basic project idea is to build a hardware (FPGA) based filter that *selectively passes traffic from one port of the Solarflare AoE card, a dual port 10Gb/s PCI-Express NIC with onboard Stratix V FPGA, to the second, sometimes filtering specific packets depending on their "session". Secondly, for traffic that belongs to a particular 'session', it will be capture and written to disk.* It is a high speed hardware-based firewall and packet capture device.

II. Basic outline & diagram

● Outline:

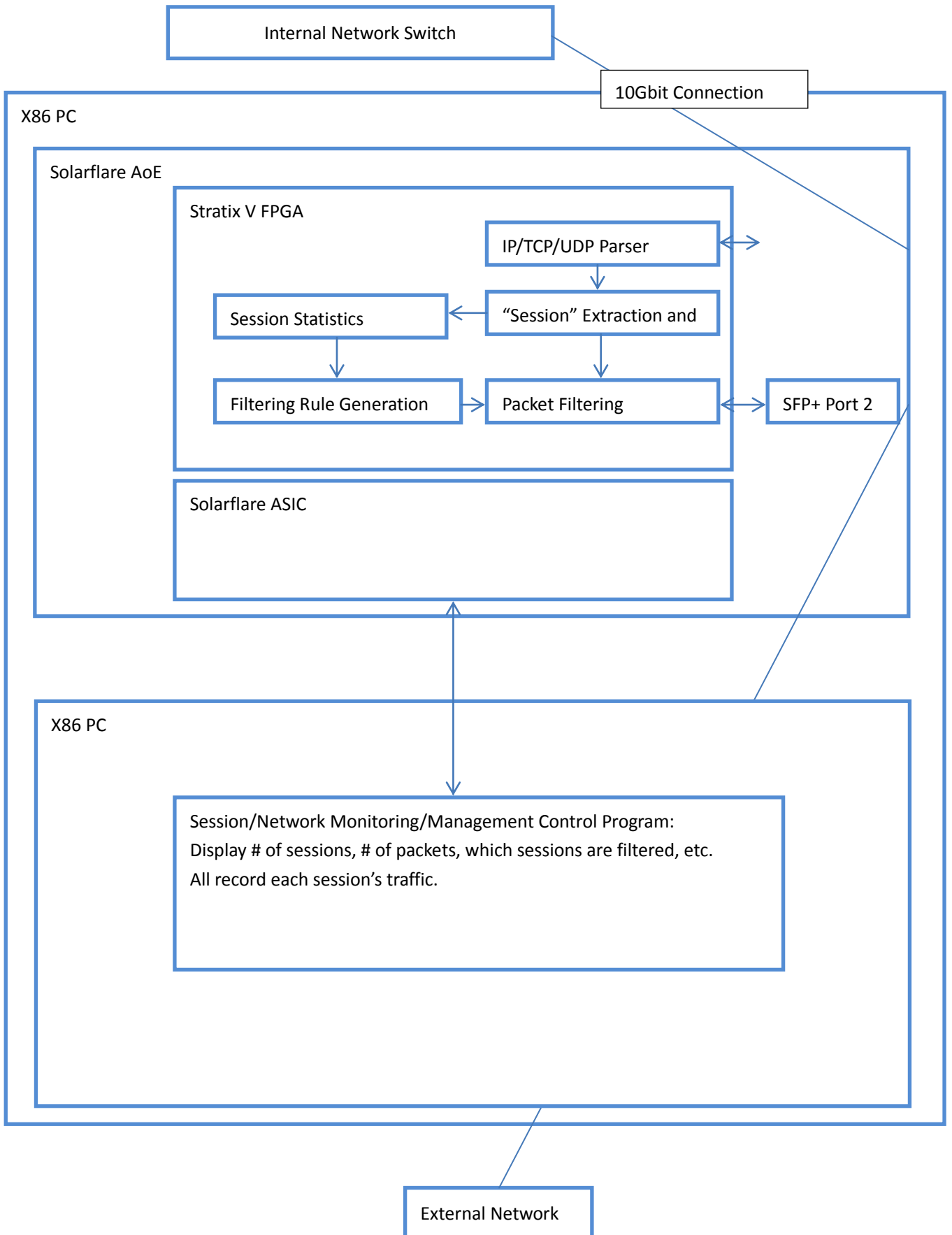
The basic outline of the project is this:

1. Outgoing packets from your network arrive at SFP+ port 1. First they are passed to the **'IP/TCP/UDP' parser**, which extracts out various parts of the packet (source and destination IP, port, protocol, and the payload).
2. Next the basic info is passed on to the **'session extractor'** which is intentionally vague. There will be several mechanisms of extracting 'sessions' from various protocols. The mechanism can be using IP hosts and ports or performing payload inspection.
3. Once the session of the packet is extracted, the data is passed both
 - 1) to the **session statistics block**: which tracks various statistics like packets sent/received per second;
 - 2) and **"packet Filtering" block**: which simply asks (using a look up table) whether the particular session's packets should be filtered or not. If the session should not be filtered, that packet is sent completely as-is out the second port of the AoE card (and on to the external network). If it is filtered, however, then the packet is simply dropped (not sent).

Optionally, the session stats can be fed into a **"rule generation"** block which changes the session filtering rules if the statistics trigger some threshold. For example, the card could start filtering any sessions that send more than 10,000 messages per second.

4. The FPGA will be communicating with regular linux software, which is used to monitor the filtering process, running on the x86 CPU. The communication between FPGA and the x86 software will be via the PCI-Express bus using the "Control Plane Interface" provided via the AOE-MM access library

● **Diagram**



III Milestones

Milestone 1 (Apr 2)

Figure out "session extractor" mechanism and its hardware solution

Finish IP/TCP/UDP Parser and packet Filtering block

Program a basic monitoring program on Linux PC for testing.

Milestone 2(Apr 16)

Finish implementing session statistics block;

Achieve the goal of recording packets to disk;

Achieve the communication between Solarflare AoE and monitoring program on Linux PC

Finish monitoring program

Milestone 3(Apr 30)

Making the system robust;

(Optionally), adding 'finance' specific to session statistics block;

(Optionally), adding a 'rule generation' block to system.