10 Gbps Line Speed Programmable Hardware for Open Source Network Applications*

Livio Ricciulli
livio@metanetworks.org
(408) 399-2284
http://www.metanetworks.org

*Supported by the Division of Design Manufacturing & Industrial Innovation of the National Science Foundation (Award #0339343) and Rome Laboratories.
Active Networks (DARPA Program)

- Change behavior of network components (routers) dynamically (add new protocols, flow control algorithms, monitoring, etc.)
  - Discrete. Update network through separate management operations.
  - Integrated. Packets cause network to update itself
- Broad scope did not result in industry adoption
  - Lack of “killer application”
  - Too much too soon
Metanetworks’ bottom-up approach

⇒ Achieve programmability reusing current infrastructure
⇒ Augment networks with non-invasive technology
⇒ Application-driven rather than design-driven
⇒ Revisit hardware computational model
10 Gbps IDS/IPS Hardware

- Open architecture to leverage open source software
  - More robust, more flexible, promotes composition
  - Directly support Snort signatures
  - Abstract hardware as a network interface from OS prospective
10 Gbps IDS/IPS Hardware (Cont.)

- Retain high-degree of programmability
  - New threat models (around the corner)
  - Extend to application beyond IDS/IPS
- Line-speed/low latency to allow integration in production networks
- Hardware support for adaptive information management
Hardware Architecture

1-10Gb

Latency < 0.5µs

>1M Concurrent Flows

1-10Gb

PHY

Block

L-1

FPGA

RAM

Read Only

Packets

< 1500

Static Policies

Synthesis + firmware update

< 100

Dynamic Policies

Compilation + runtime update

IPS/IDS

State
Flynn’s Computer Taxonomy

**MIMD**
- Instructions
- Data
- Memory
- Processor

**MISD**
- Data
- Alert
- Reduction Network
- Instructions

**SISD**
- Instructions
- Data
- Memory
- Processor

**SIMD**
- Data
- Alert
- Reduction Network
- Instructions

**Reduction Network**
- P0
- P1
- ... Pn
MISD Programmable Hardware

FPGA

Stateful Analysis

Reduction Network

R1 R2 .... Rn

Receive Clock

Data Valid

Data Stream

Match Memory

Host Interface
Static analysis of large number of IDS signatures

- Transform Snort rules or BPF expressions into a low-level declarative language
- Extract fine-grain parallelism across thousands of signatures
  - Define independent FSMs each implementing a signature
  - Share comparison logic across multiple FSMs
- Synthesizer further optimizes
  - Merge multiple FSMs sharing intermediate states
  - Eliminate redundant rules
10Gbps Information bandwidth management

► Host bandwidth is approximately 1/100th of fast-path
  ⇒ Flooding not to be used to compromise blocking capability 😊
  ⇒ Flooding can be exploited to reduce efficacy of monitoring 😞

► Need to find needle in a haystack but needs to cope with flood of packets
  ⇒ Hardware stateful analysis (implemented)
  ⇒ Intelligent Monitoring
  ⇒ Application-level programmability
Intelligent Monitoring (work in progress)

\[ \Sigma > T? \]

Switch off lower priority rules and report number of triggers only (NOT entire packet).

\[ T = \text{maximum amount of alerts tolerable} \]
Application-level programmability

► API to let user write ad-hoc wire-speed code
► Data parallel architecture provides determinism
  ⇒ It either fits or it does not fit in the FPGA
  ⇒ It either meets timing or does not meet timing
  ⇒ Load/store network processing much harder to predict
Summary

► Bottom-up design approach promising in delivering line speed hardware programmability
► Extremely low latency design enables a wide variety of deployment options
► Can (cost-effectively) scale to 10 Gbps Ethernet
► Processing paradigm lends itself to ad-hoc application level programmability
► More work needed in hardware support for effectively managing floods of information
► Much work needed to support composability

Livio Ricciulli
livio@metanetworks.org
(408) 399-2284
www.metanetworks.org