Application-Oriented Network Traffic Analysis Tool based on GPUs

P. DeMar, W. Wu, L. Zhang (Fermilab)

Fermilab

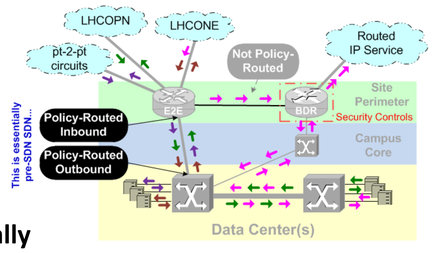
An Alternate Approach for Driving Software-Defined Networking (SDN)

U.S. DEPARTMENT OF ENERGY

Problem Space

Fermilab has a long-standing strategy to isolate high-impact WAN traffic from general internet traffic

- Separates elephant flows (bulk data movement) from interactive & jitter-sensitive traffic
- Currently accomplished through dedicated network infrastructure and Policy-Based Routing (PBR)
- Dedicated infrastructure is expensive, inefficient, inflexible



Emerging Software-Defined Network (SDN) technologies potentially offer dynamic network configurability options

- Partition of network infrastructure into "slices" for specific traffic flows (ie., isolation)
- Customized allocation of network resources as well (ie., bandwidth)

But how should dynamic SDN network configurations be facilitated?

- Manual reconfiguration is inherently static & doesn't scale well to complex traffic patterns
- Application-driven reconfiguration would be an efficient on-demand approach that scales
  - But requires network-awareness built into applications
  - Increases software adaptation & maintenance burdens on developers

Proposed Solution

Our solution – Let the network react to specific traffic flows by reconfiguring itself

Fermilab is developing a network traffic analyzer tool to detect "special" traffic flows

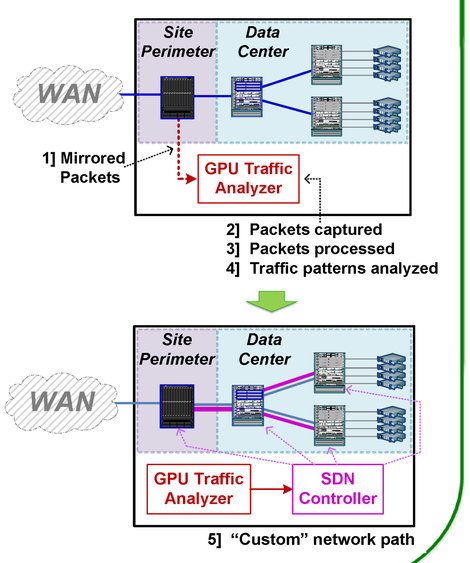
- Based on real-time packet analysis
- Output to modify (SDN) network path characteristics
- A Laboratory-Directed R&D (LDRD) project

Tool provides two distinct functions

- High-performance packet capture function
  - Designed for 40GE/100GE network environments
- GPU-based network traffic pattern recognition algorithms
  - Generic GPU libraries for packet manipulation
  - Custom GPU libraries for traffic identification

Why GPUs?

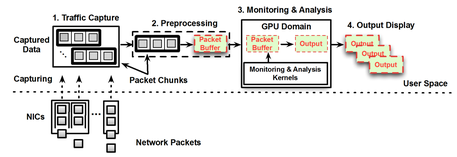
Features	NPU/ASIC	CPU	GPU
Easy programmability	✕	✓	✓
High compute power	Depends	✕	✓
High memory bandwidth	Depends	✕	✓
Data-parallel execution model	✕	✕	✓



Tool Design & Components

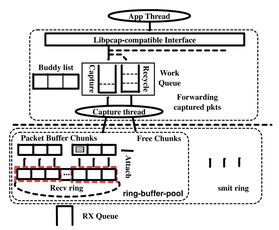
Our network traffic analysis tool has four logical components:

1. Packet Capture
2. Packet Preprocessing
3. Traffic Analysis
4. Output {SDN controller (re)configuration}



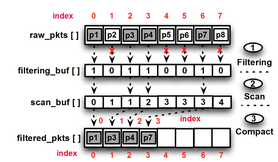
Packet Capture Engine

- Design goal is lossless packet capture
- Memory mapping-based zero copy
- Novel ring buffer management scheme for short-term load imbalance
- Unique offload mechanism to avoid long-term load imbalance
- (Re)transmit function to allow potential use as a middle-box engine



GPU-assisted Processing & Packet Analysis

GPU-accelerated libraries for packet analysis and flow identification:

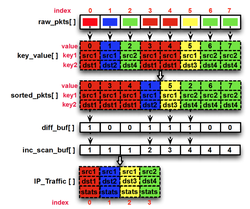


Packet-Filtering Kernel:

- Analyzes only packets of interest
- Uses BKF

Traffic-Aggregation Kernel:

- Aggregates packets with same src/dest addresses & ports
- Provides statistics at the flow-level



Status

Packet capture component completed:

- Using 10GE NICs (40GE NIC support soon)
- Available as stand-alone software package (WireCap.fnal.gov)

GPU processing component in prototype testing:

- Production-quality software development currently in progress

Product road map:

- Integrated beta prototype in summer '15
- Analysis module completed in winter '16
- SDN controller interface in summer '16

Wider Applicability

Strategic design objective – Develop a generic platform for wider applicability

Design Requirements:

- Lossless packet capture engine
- Capability for deep packet analysis
- Multiple NIC support
- Advanced NIC support (40GE/100GE)
- Retransmit function

Potential application areas:

- Packet-based security tools
- Middle-box devices & appliances
- Real-time flow performance analysis