NFQL

(Network Flow Query Language)

nfql.vaibhavbajpai.com

Vaibhav Bajpai

AN 2012

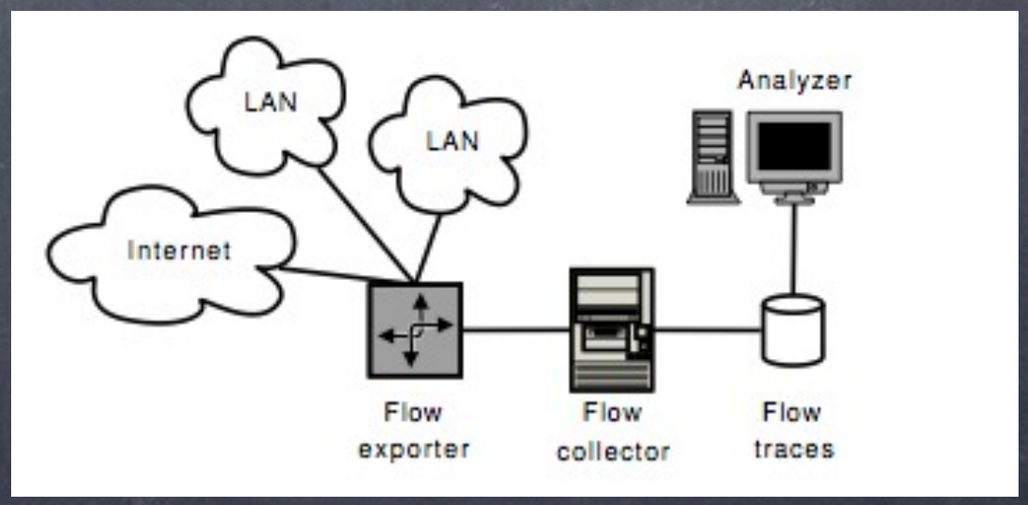
Overview

- Precursor Introduction
- NFQL Demo and NFQL internals discussion
- NFQL applications
- Experiences, Lessons Learned
- Contribute

Precursor

- What are network flows?

  a sequence of packets sent from a particular source to a particular unicast, anycast, or multicast destination that the source desires to label as a flow. [1]



[1] RFC 3697

Precursor

- Flow Export Protocols
  - Cisco Netflow

    7-tuple flow-key, namely:

    {srcIP, dstIP, srcPort, dstPort, ipProto, ifIndex, ipTOS}
  - IETF IPFIX

version	features
v1, {2, 3, 4}	original format with several internal releases
v5	CIDR, AS support and flow sequence numbers
v{6, 7, 8}	router-based aggregation support
v9	template-based with IPv6, and MPLS support
IPFIX	universal standard, transport-protocol agnostic

Precursor

- Flow Analysis Tools
  - flow-tools
  - nfdump
  - SiLK
  - NFQL

NFQL

- Evolution
  - Query Language Specification [2009]

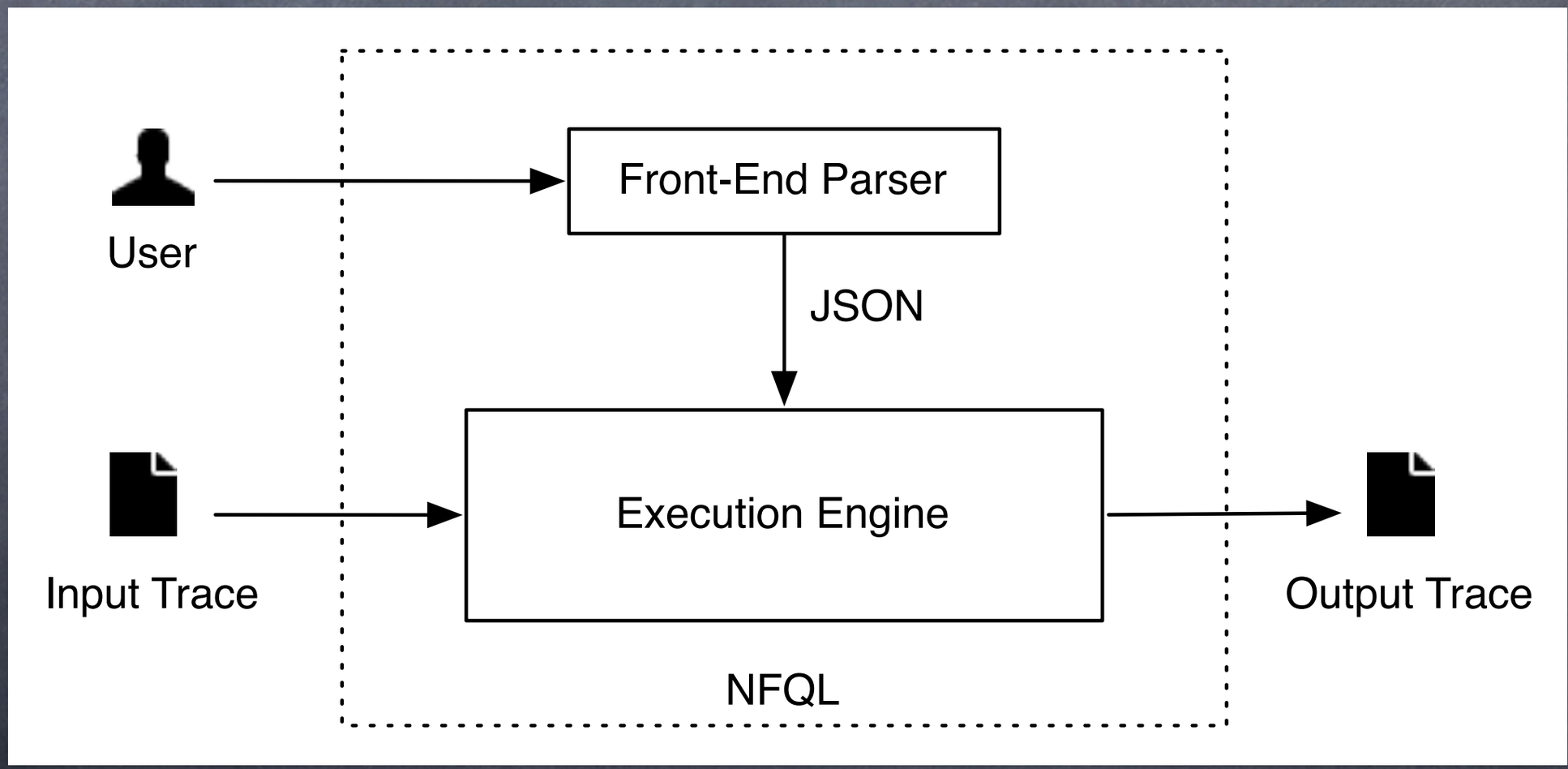
python
- Flowy: First Prototype [2009]
- Flowy with Map Reduce (Investigative) [2010]

c
- F (v1) [2011]
- NFQL [2012]

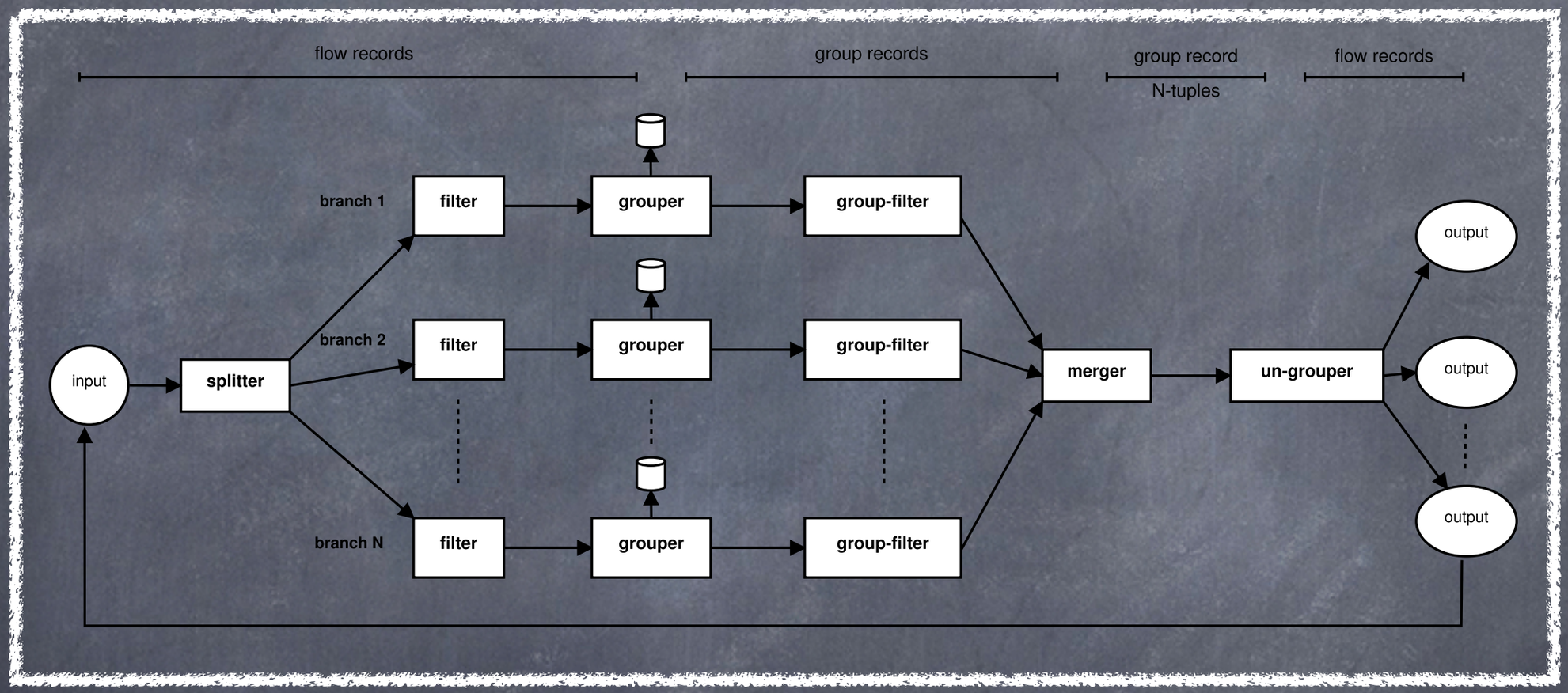
Number of records	Flowy	F (v1)
103k	1177s	0.3s
337k	20875s	3.4s
656k	70035s	13s
868k	131578s	23s
1161k	234714s	86s

NFQL

- Architecture



NFQL



- filter flow-records
- combine them into groups
- apply relative filters
- aggregate their flow-fields
- invoke allen interval algebra

Demo

internals discussion

Applications

- Application Signatures [IM 2011]
- IPv6 Transition Failure Identification [AIMS 2012]
- Cybermetrics [AIMS 2010]

Evaluations
(filter)

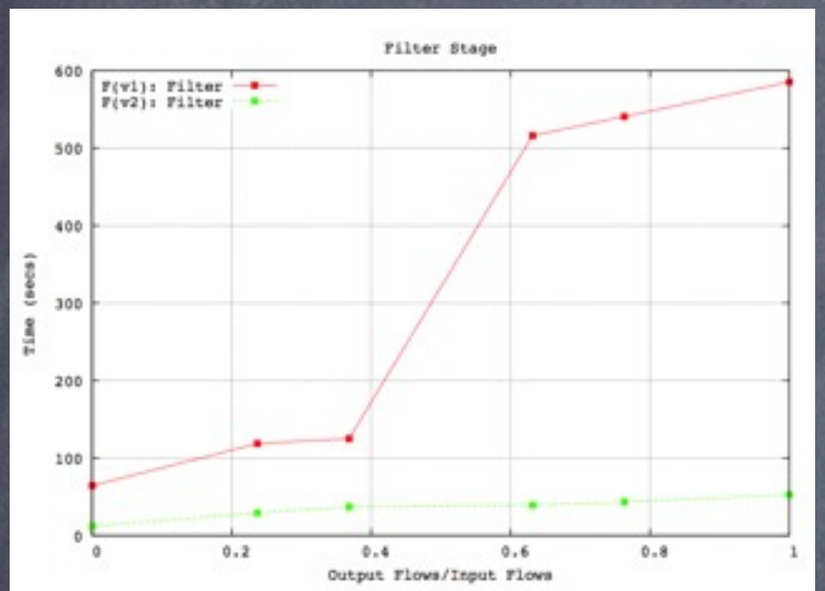


Figure 22: Filter Stage: F(v1) vs F(v2)

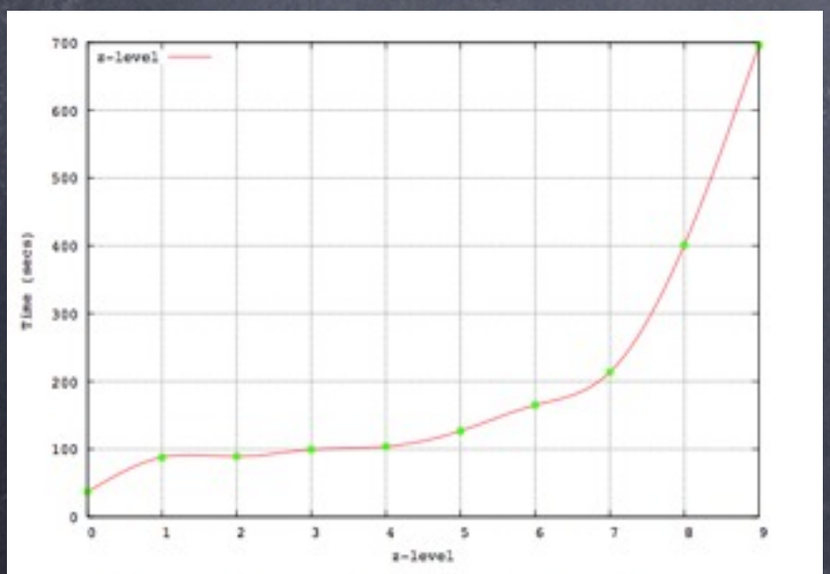


Figure 21: F(v2): `z-level` Effect on Performance

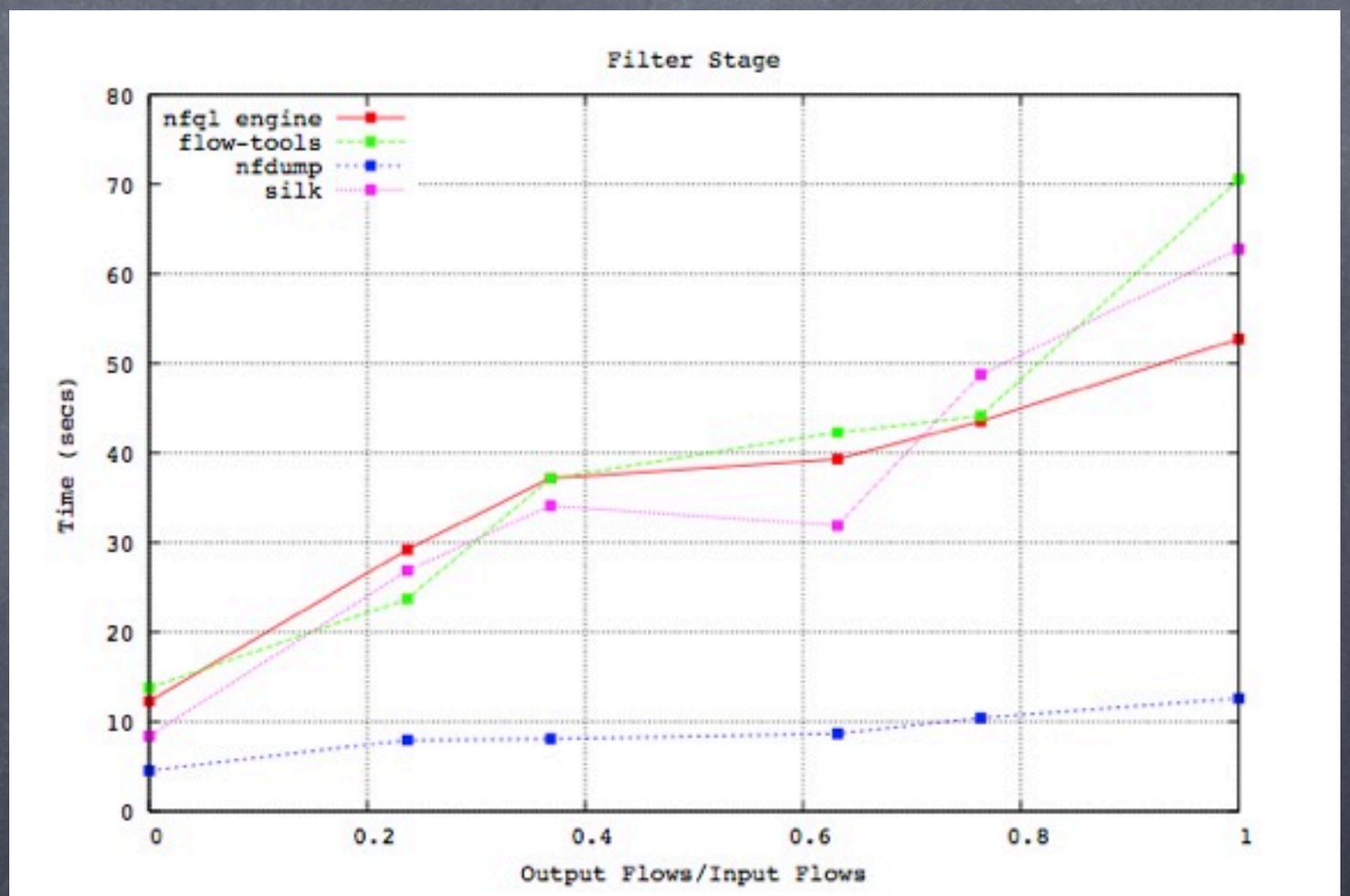


Figure 26: Filter Stage: NFQL vs SiLK, Flow-Tools, Nfdump

Lessons Learned

- evolving a project is harder than starting from scratch
- continuous feedback loop is always good
- focus attention on areas that will have more impact
- do performance evaluations early
- test-first development

How can you help?

- Look into the Issue Tracker [1]
- Future Work:
  - IPFIX support
  - mmap tracefile, multithreaded filter
  - lzo compression support
  - parallelized grouper qsort
  - hash table lookups
  - extend regression test-suite with more test-cases

[1] https://github.com/vbajpai/nfql/issues

Voluntary Assignment

- Download and compile NFQL [1]
- Create a new query and run on it on your flows
- If you find a bug, please report it

[1] nfql.vaibhavbajpai.com