pmacct and Streaming Telemetry

Paolo Lucente

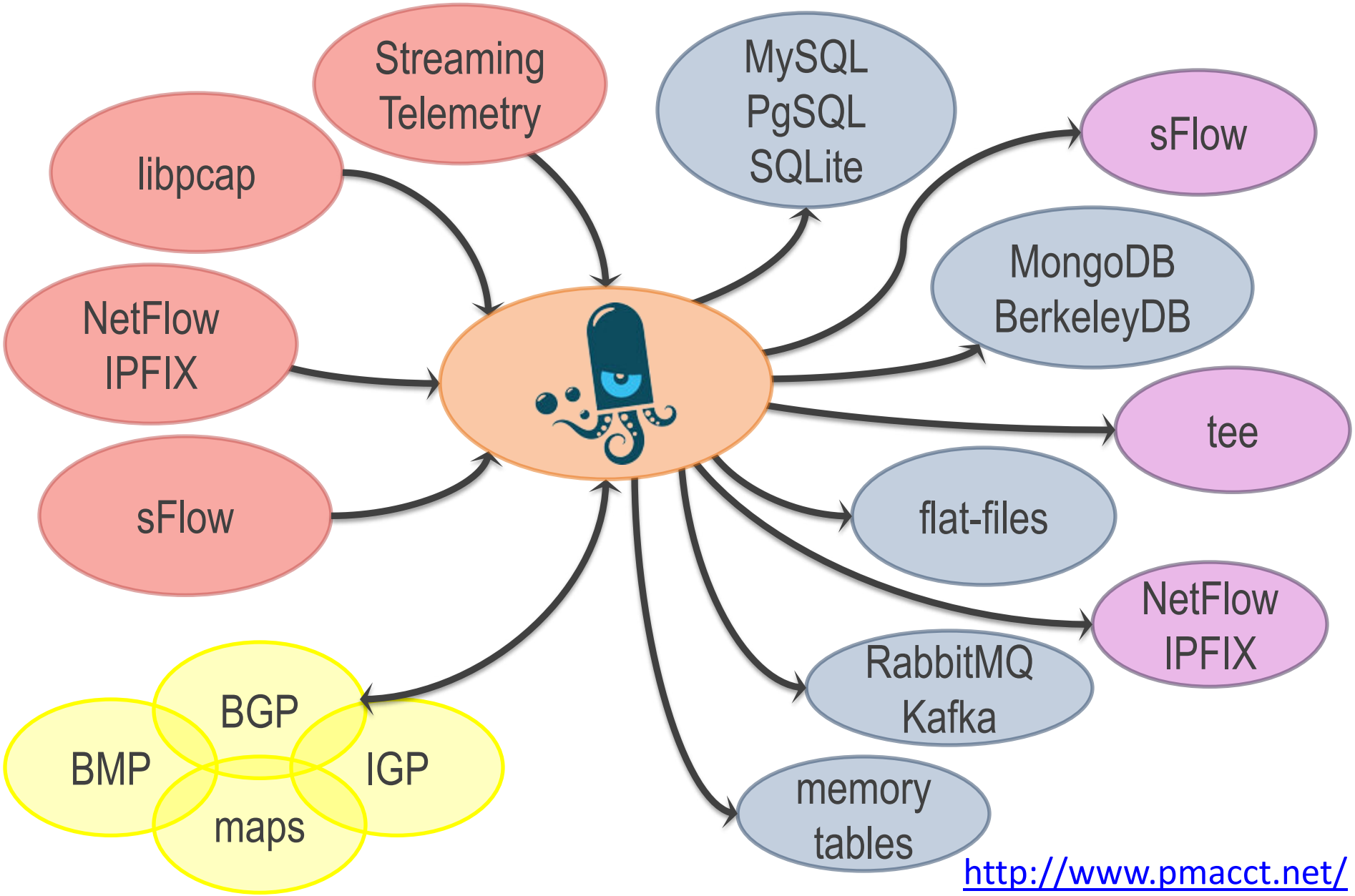
pmacct

NLNOG Day 2016, Amsterdam – Sep 2016

whoami: Paolo

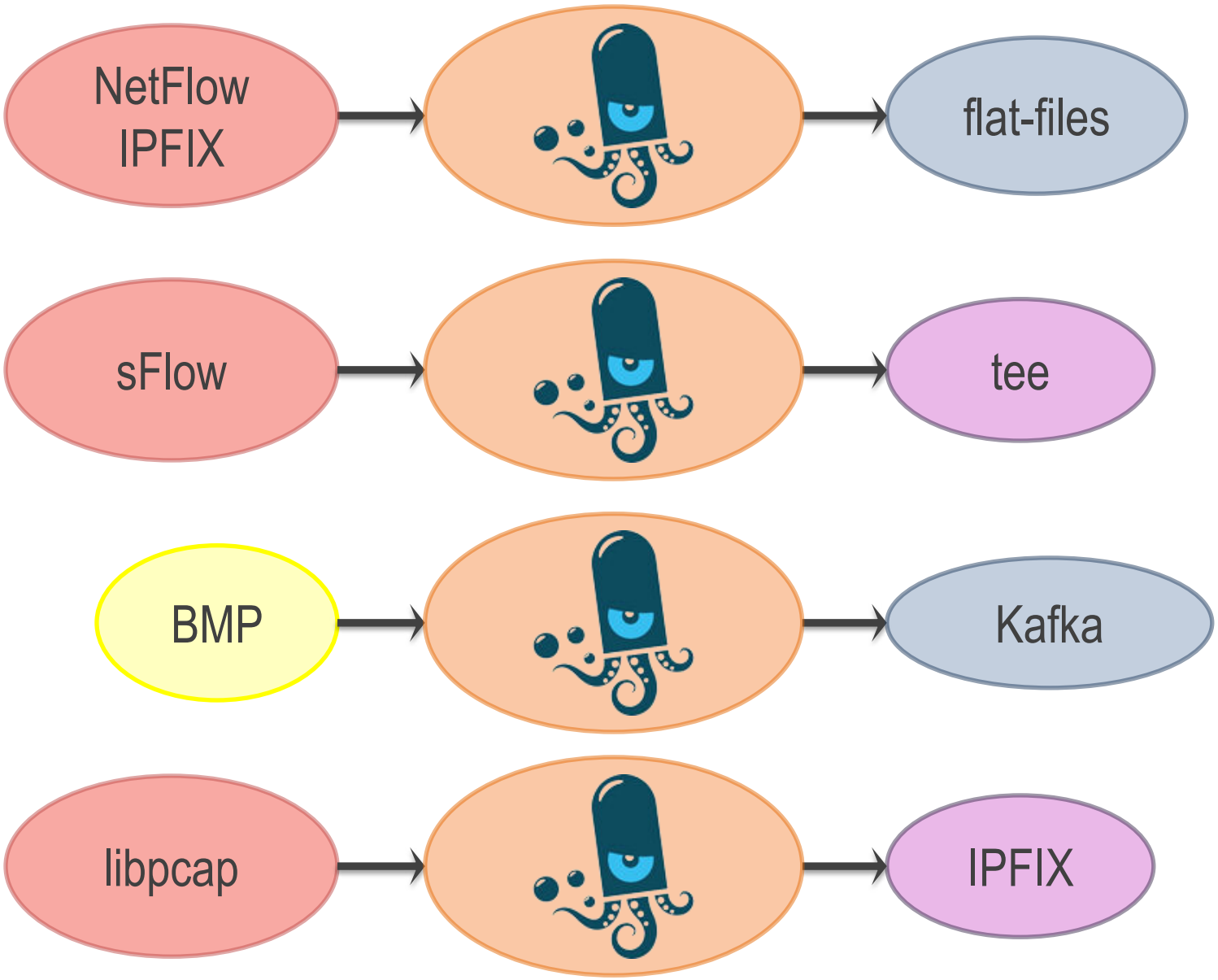
- Been originally working for operators for a while
- Been working for vendors for a little while after that
- Been involved with IP accounting for a while
  - Hence I stumbled upon NetFlow in the 90's ☺
- Within operators, network traffic telemetry is beneficial in several contexts, ie.:
  - Traffic engineering
  - Capacity planning
  - Peering
  - …
  - and also *(ie. not only)* security

pmacct is open-source, free, GPL'ed software

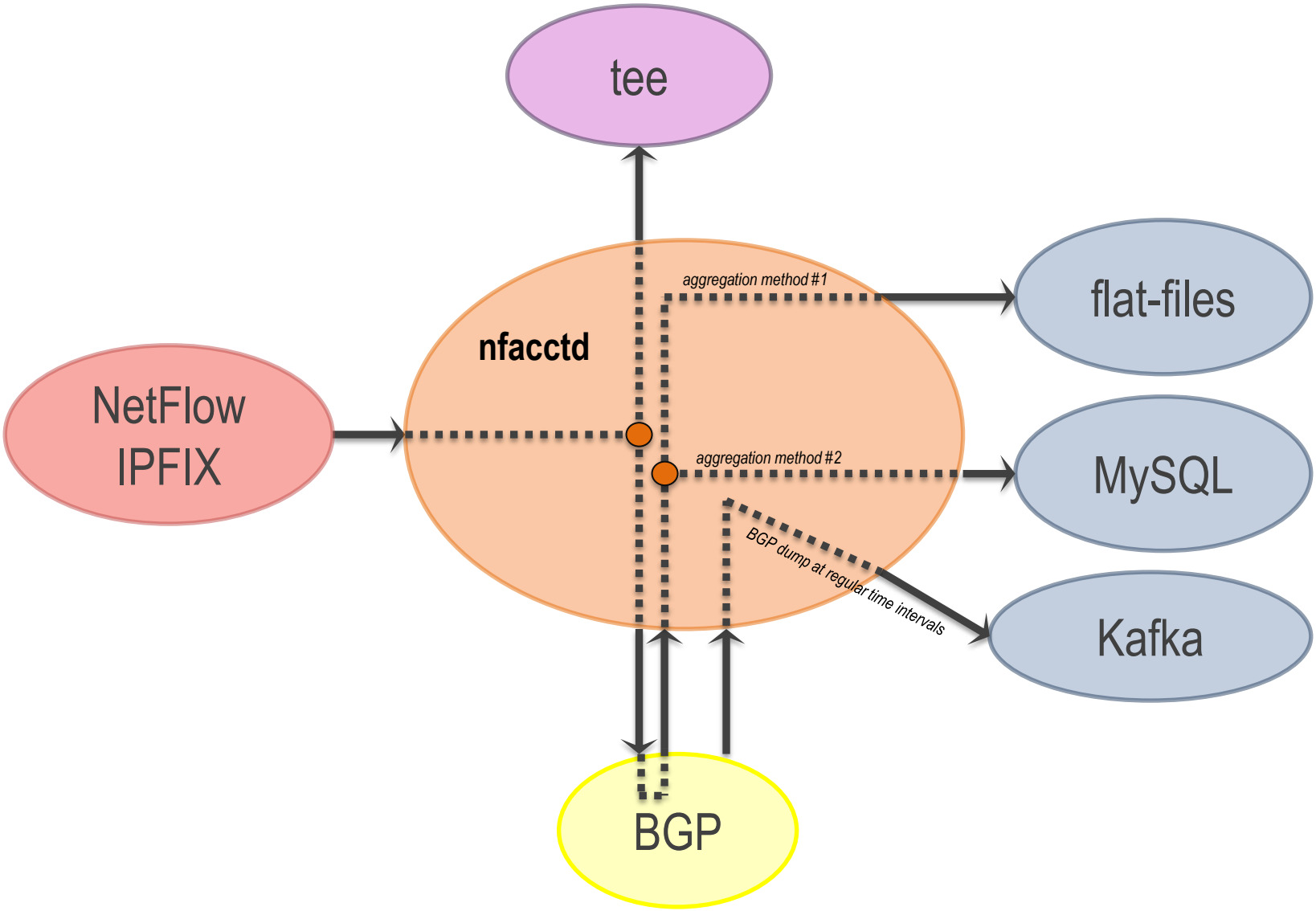


http://www.pmacct.net/

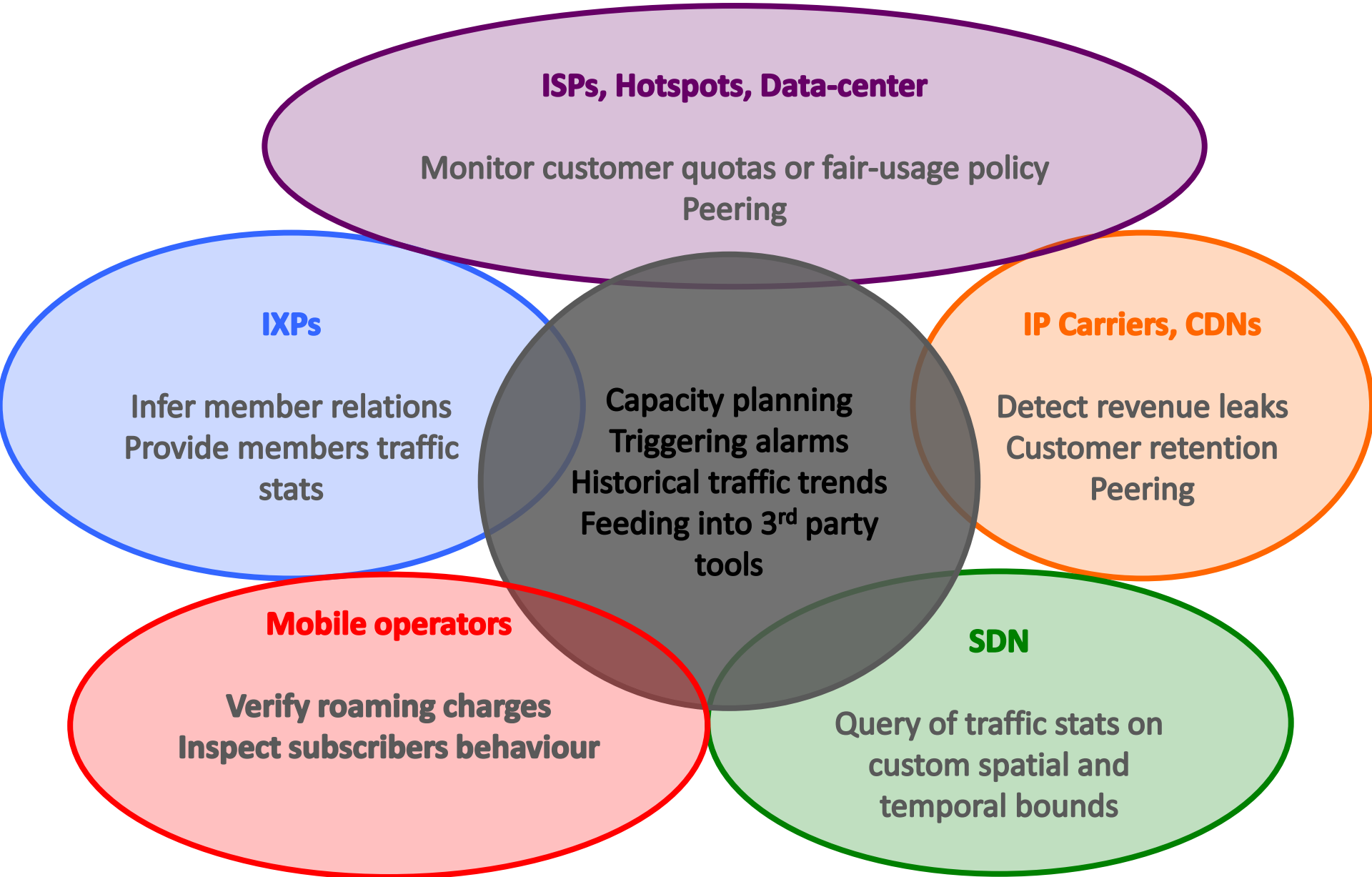
pmacct: a few simple use-cases



pmacct: one slightly more complex use-case



Usage scenarios



Key pmacct non-technical facts

- 10+ years old project
- Can’t spell the name after the second drink
- Free, open-source, independent
- Under active development
- Innovation being introduced
- Well deployed around, also large SPs
- Aims to be the traffic accounting tool closer to the SP community needs

Some technical facts (1/2)

- Pluggable architecture:
  - Can easily add support for new data sources and backends
- Correlation of data sources:
  - Natively supported data sources (ie. BGP, BMP, IGP, Streaming Telemetry)
  - External data sources via tags and labels
- Pervasive data-reduction techniques, ie.:
  - Data aggregation
  - Filtering
  - Sampling

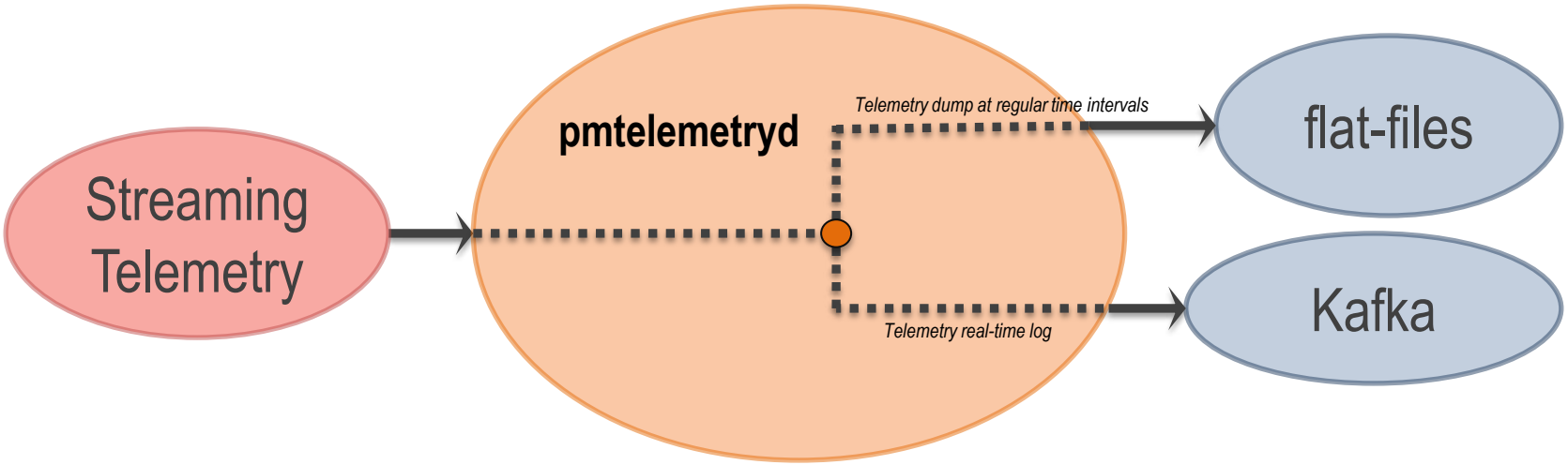
Some technical facts (2/2)

- Build multiple views out of the very same collected network traffic dataset , ie.:
  - Unaggregated to flat-files for security and forensics; or to message brokers (RabbitMQ, Kafka) for Big Data
  - Aggregated as [<ingress router>, <ingress interface>, <BGP next-hop>, <peer destination ASN>] and sent to a SQL DB to build an internal traffic matrix for capacity planning purposes
- Enable analytics against the collected data sources (ie. BGP, BMP, Streaming Telemetry):
  - Stream real-time
  - Dump at regular time intervals (possible state compression)

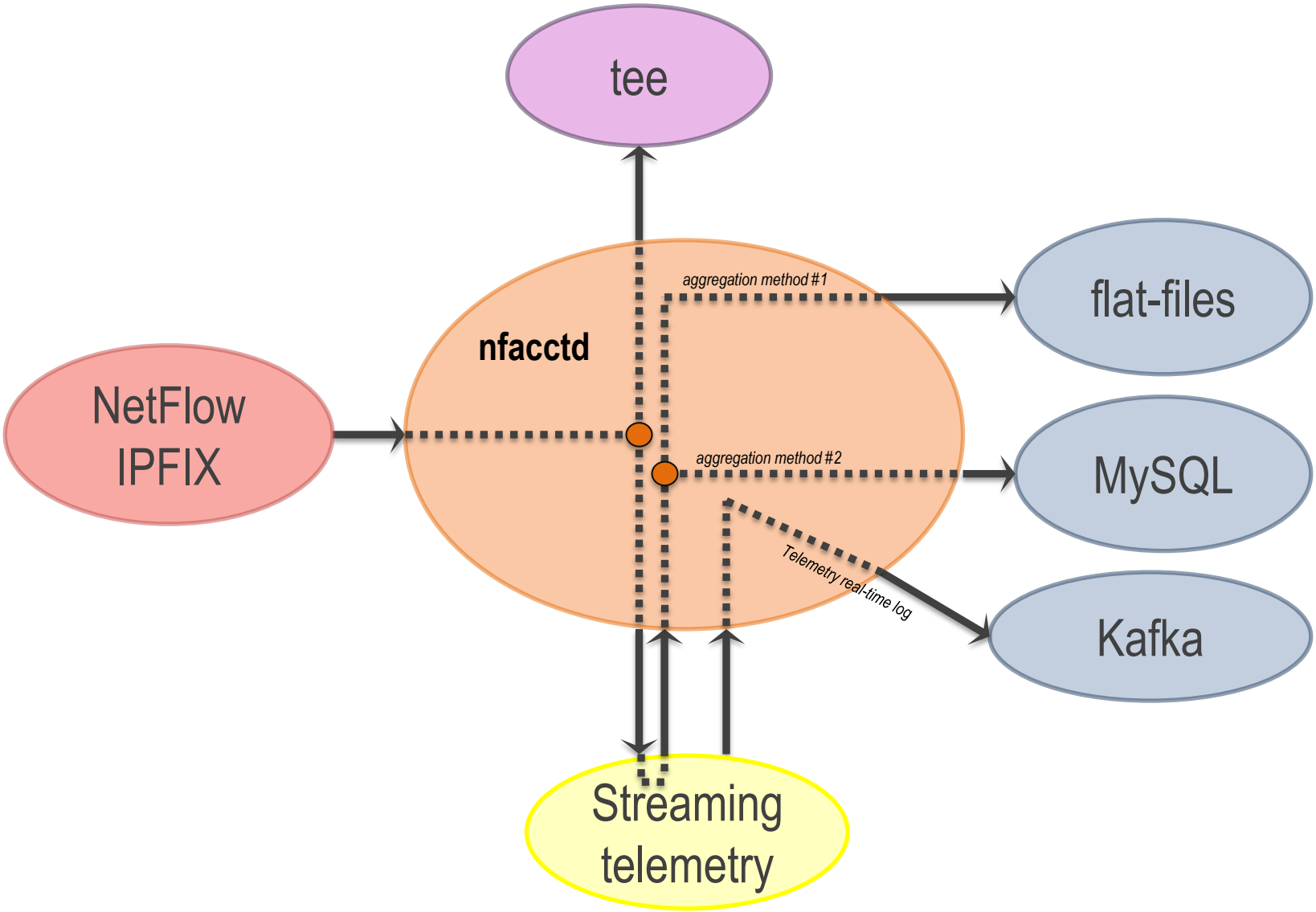
Streaming Telemetry

- Summarizing Cisco IOS-XR Telemetry Configuration Guide (at the time of this writing):
  - Streaming Telemetry lets users direct data to a configured receiver
  - This is achieved by leveraging the capabilities of M2M communication
  - The data is used by DevOps people to optimize networks by collecting analytics of the network in real-time

pmacct & Streaming Telemetry (1/2)



pmacct & Streaming Telemetry (2/2)



<rant>

Streaming Telemetry

- Been so far an exciting experience of delving into an enchanted, non standardized world:
  - Data modelling is cool:
    - Standardization focuses on this part
  - Transport, subscription mechanisms, data serialization are not cool enough apparently:
    - Data is known to spontaneously migrate
    - And then get magically decoded
    - Things like that, “details” ..

Streaming Telemetry

- Having myself deep roots in the Service Providers community, I do believe in the mantra "*Operators should get more involved in standardization*"
- But now look at:
  - http://www.openconfig.net/projects/streaming-telemetry/
  - http://www.openconfig.net/about/participants/
  - This does feel a bit like revenge, doesn't it?

Streaming Telemetry

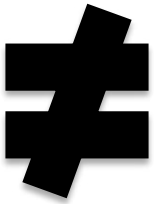
- Homework: figure out your own practical examples when it comes to “details” (some keywords as hint: gRPC, netconf, restconf, JSON, GPB, Avro)
- Fun fact: GPB requires inclusion of source code to work: was it not that when you do that, licensing of code starts to kick in?
- Quote from the industry: “Let’s hope they don’t turn out into the enterprise MIBs of the 21st century” (David Barroso)

Streaming Telemetry

This is all with still little adoption (maybe PoC’s?) outside the circle of the Big Guys

How is

A peaceful gathering of Vendors



≠

(as in any worse)

than

An Operators (only!) Working Group

?

(Btw, this is a rare picture of Vendors holding breath during an Operators Working Group meeting ☺)

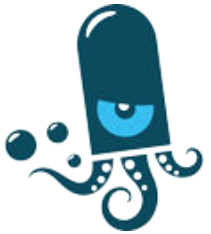
Streaming Telemetry

- Steaming Telemetry has great potential
- For some aspects of it, fragmentation flag is on
  - Fragmentation as in: “several equivalent choices”
- Who benefits from fragmentation?
- Let’s not take abstraction as the excuse

</rant>

Further information about pmacct

- https://github.com/pmacct/pmacct
  - Official GitHub repository, where star and watch us ☺
- http://www.pmacct.net/lucente_pmacct_uknof14.pdf
  - More about coupling telemetry and BGP
- http://ripe61.ripe.net/presentations/156-ripe61-bcp-planning-and-te.pdf
  - More about traffic matrices, capacity planning & TE
- http://wiki.pmacct.net/ImplementationNotes
  - Implementation notes (RDBMS, maintenance, etc.)



pmacct and Streaming Telemetry

Thanks! Questions?

Paolo Lucente <paolo@pmacct.net>