



# Latests on BGP monitoring

Paolo Lucente

NTT Communications | pmacct

# whoami

Paolo Lucente

GitHub: [paololucente](#)

LinkedIn: [plucente](#)



Digging telemetry data out of networks worldwide for fun and profit since I had no white hairs in my beard.

# BGP

- Protocol to advertise Reachability Information:
  - The Network Layer part of the story, while still dominant, is “old”: BGP is, in fact, used as transport for a variety of different info (\*)
- Good at policy control:
  - Even though it must be noted that metrics like latency, jitter and packet loss are increasingly popular for content delivery in place of the traditional BGP selection algorithm
- Superlative at information hiding:
  - But, then again, this is the recipe for scaling to the current Internet size and beyond

(\*) Playing Battleships over BGP : <https://blog.benjojo.co.uk/post/bgp-battleships>

# Early attempts at gaining visibility

## On BGP ADD-PATHS

- BGP ADD-PATHS covers several use cases:
  - Mostly revolving around actual routing
  - Extra path flooding questioned in such context (\*)
- Our use-case for BGP ADD-PATHS is around monitoring applications:
  - Not much talk yet in such context
  - Proposal to mark best-paths to benefit monitoring applications: draft-bgp-path-marking (Cardona et al.)

(\*) [http://www.nanog.org/meetings/nanog48/presentations/Tuesday/Raszuk\\_To\\_AddPaths\\_N48.pdf](http://www.nanog.org/meetings/nanog48/presentations/Tuesday/Raszuk_To_AddPaths_N48.pdf)

## pmacct and BGP ADD-PATHS

- In early Jan 2014 pmacct BGP integration got support for BGP ADD-PATHS
  - GA as part of 1.5.0rc3 version (Apr 2014)
- Why BGP ADD-PATHS?
  - Selected over BMP since it allows to not enter the exercise of parsing BGP policies
  - True, post-policies BMP exists but it's much less implemented around and hence not felt the way to go

24

- Circa 2013
- Goal: see all paths in a BGP multi-path scenario, avoiding screen scraping

Credits to: E. Jasinska (Netflix), P. Lucente (pmacct) @ NANOG61

# BMP

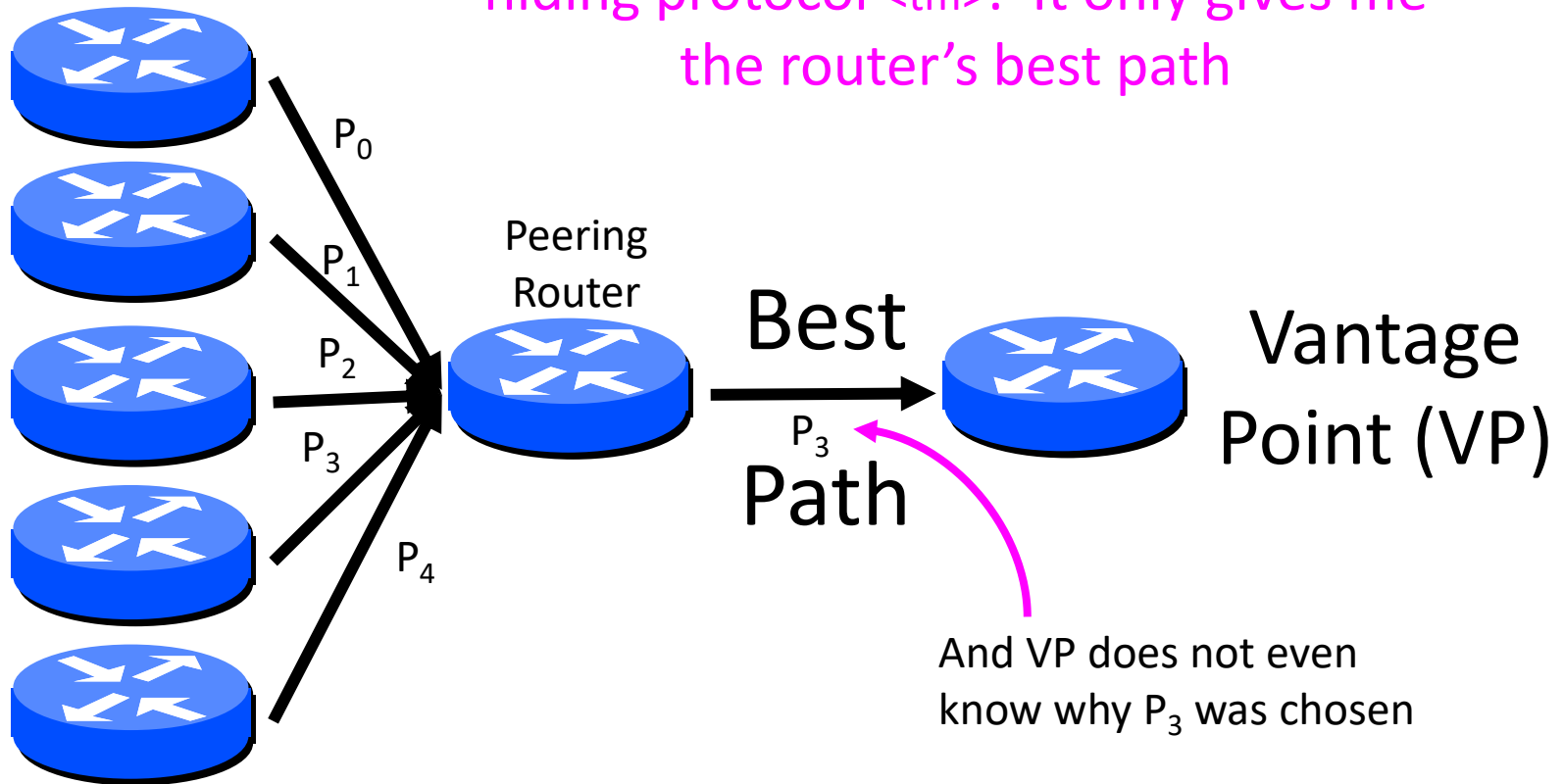
- BGP Monitoring Protocol
- RFC 7854:
  - first draft in 2008, sparse work until 2012;
  - stall between 2012 and 2015;
  - real traction kicks in: 10 drafts between 2015 and 2016;
  - RFC award in Jun 2016
- Uncomplicated protocol design 
- Great effort but ..
  - .. industry evolved all these years
  - increased hunger for data



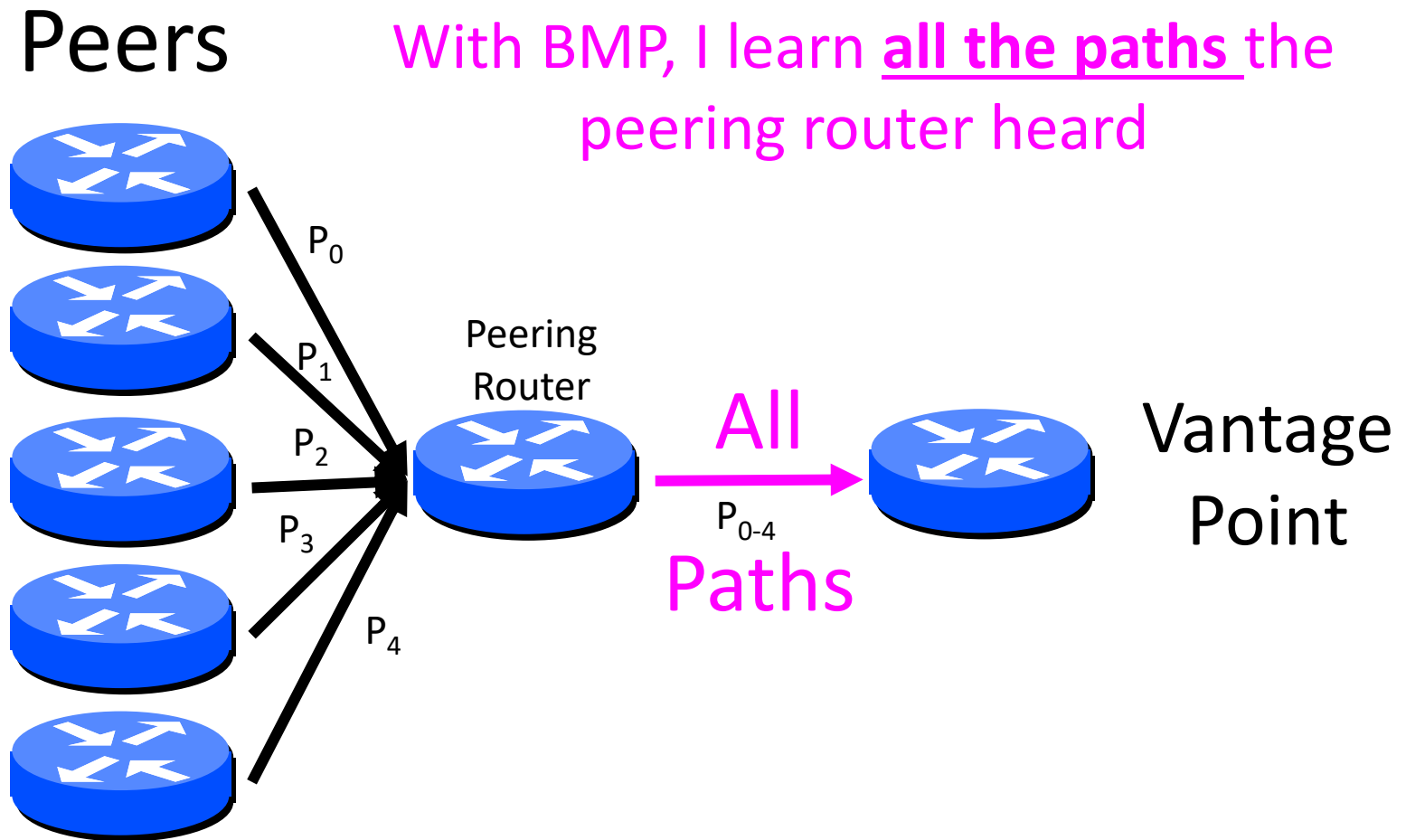
A DevOps guy during lunch break

# Traditional BGP monitoring

Peers



# BGP monitoring with BMP (1/2)



# BGP monitoring with BMP (2/2)

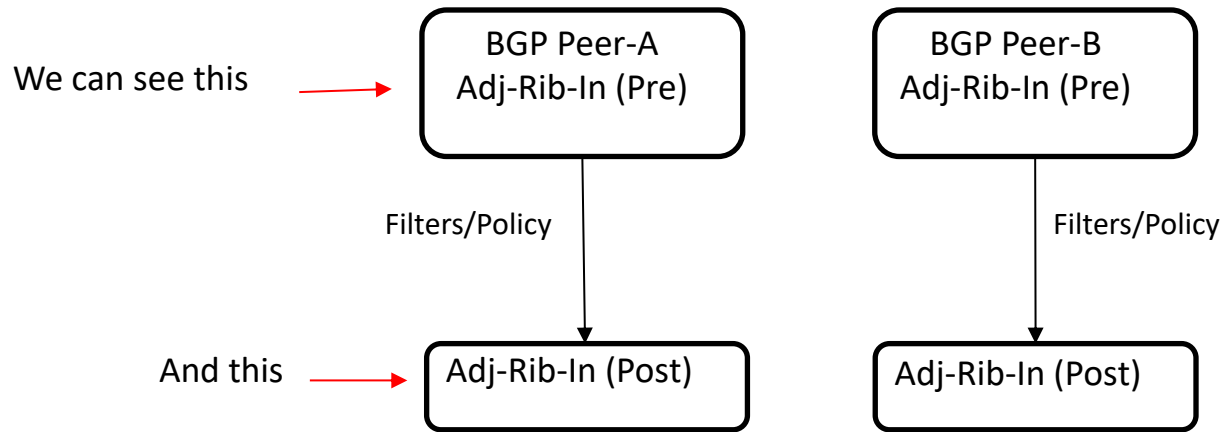
- o Message Type (1 byte): This identifies the type of the BMP message. A BMP implementation MUST ignore unrecognized message types upon receipt.
  - \* Type = 0: Route Monitoring
  - \* Type = 1: Statistics Report
  - \* Type = 2: Peer Down Notification
  - \* Type = 3: Peer Up Notification
  - \* Type = 4: Initiation Message
  - \* Type = 5: Termination Message
  - \* Type = 6: Route Mirroring Message



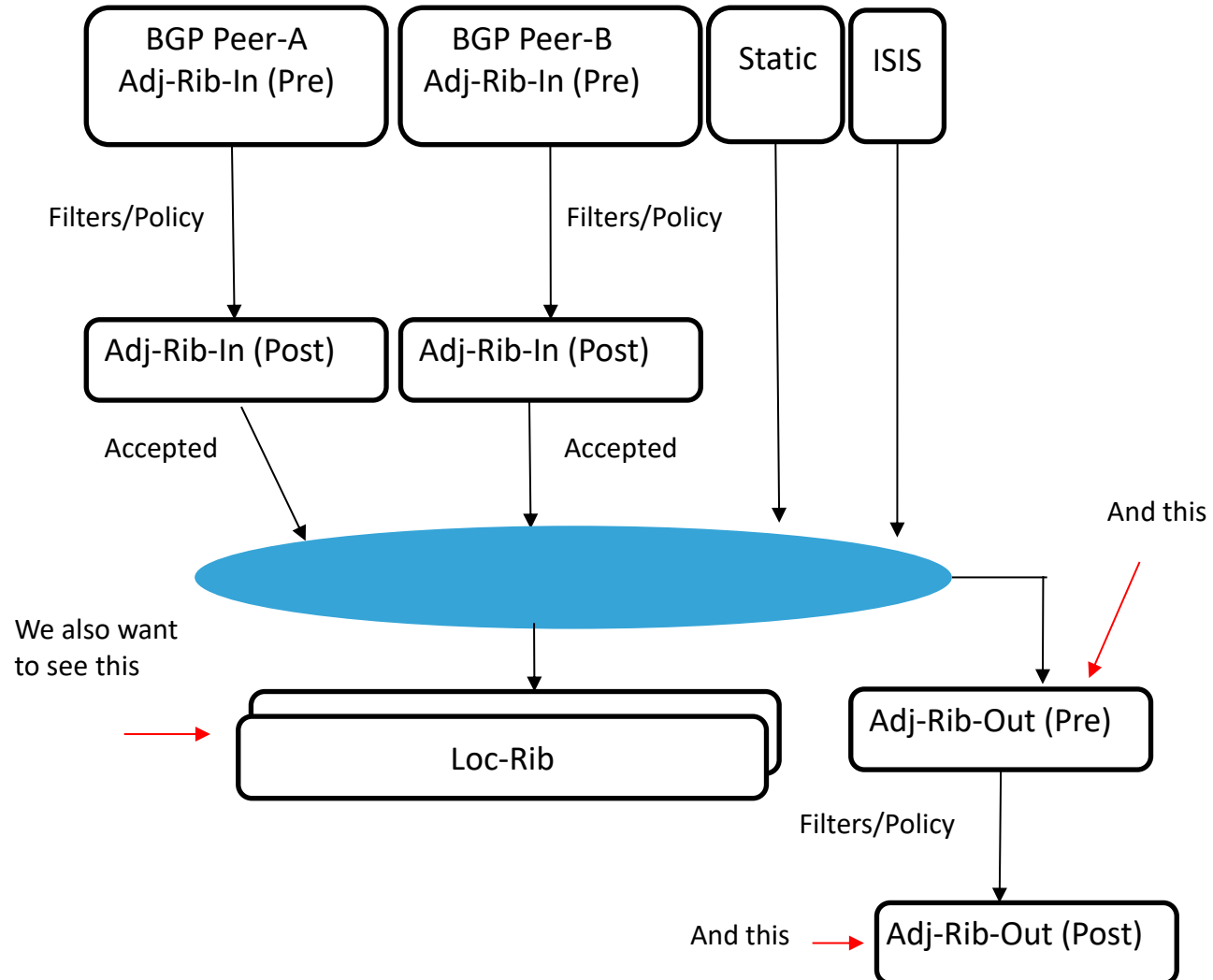
# BMP: problem statement

- The BGP protocol is one of the very few protocols running on the Internet that has a standardized, clean and separate monitoring plane, BMP (think, for example, to DNS ..)
- BMP, in its current shape, does cover only pre- and post- policies Adj-RIB-In; an operator would still worse-case need:
  - Actual BGP peering(s) for loc-RIB
  - Screen scraping for Adj-RIB-Out

# Problem statement visualized



# Proposal: extend BMP to loc-RIB and Adj-RIB-Out (1/3)



Credits to: T. Evens (Cisco), S. Bayraktar (Cisco), P. Lucente (NTT) @ GROW WG, IETF 98

# Proposal: extend BMP to loc-RIB and Adj-RIB-Out (2/3)

Global Routing Operations  
Internet-Draft  
Updates: 7854 (if approved)  
Intended status: Standards Track  
Expires: September 3, 2018

T. Evens  
S. Bayraktar  
Cisco Systems  
P. Lucente  
NTT Communications  
P. Mi  
Tencent  
S. Zhuang  
Huawei  
March 2, 2018

Support for Adj-RIB-Out in BGP Monitoring Protocol (BMP)  
draft-ietf-grow-bmp-adj-rib-out-01

## Abstract

The BGP Monitoring Protocol (BMP) defines access to only the Adj-RIB-In Routing Information Bases (RIBs). This document updates the BGP Monitoring Protocol (BMP) RFC 7854 by adding access to the Adj-RIB-Out RIBs. It adds a new flag to the peer header to distinguish Adj-RIB-In and Adj-RIB-Out.

# Proposal: extend BMP to loc-RIB and Adj-RIB-Out (3/3)

Global Routing Operations  
Internet-Draft  
Updates: 7854 (if approved)  
Intended status: Standards Track  
Expires: August 27, 2018

T. Evens  
S. Bayraktar  
M. Bhardwaj  
Cisco Systems  
P. Lucente  
NTT Communications  
February 23, 2018

Support for Local RIB in BGP Monitoring Protocol (BMP)  
draft-ietf-grow-bmp-local-rib-01

## Abstract

The BGP Monitoring Protocol (BMP) defines access to the Adj-RIB-In and locally originated routes (e.g. routes distributed into BGP from protocols such as static) but not access to the BGP instance Loc-RIB. This document updates the BGP Monitoring Protocol (BMP) RFC 7854 by adding access to the BGP instance Local-RIB, as defined in RFC 4271 the routes that have been selected by the local BGP speaker's Decision Process. These are the routes over all peers, locally originated, and after best-path selection.

# draft-ietf-grow-bmp-{local-rib,adj-rib-out} use-cases

- Loc-RIB:
  - Monitor routes selected and used by the router:
    - ECMP
    - Correlation with NetFlow/IPFIX
    - Next-hop preservation
  - Monitor locally originated and BGP routes without requiring a BGP peering
  - Policy verification
- Adj-RIB-Out:
  - Monitor routes advertised to peers
  - Policy verification

# draft-ietf-grow-bmp-{local-rib,adj-rib-out} standardization status

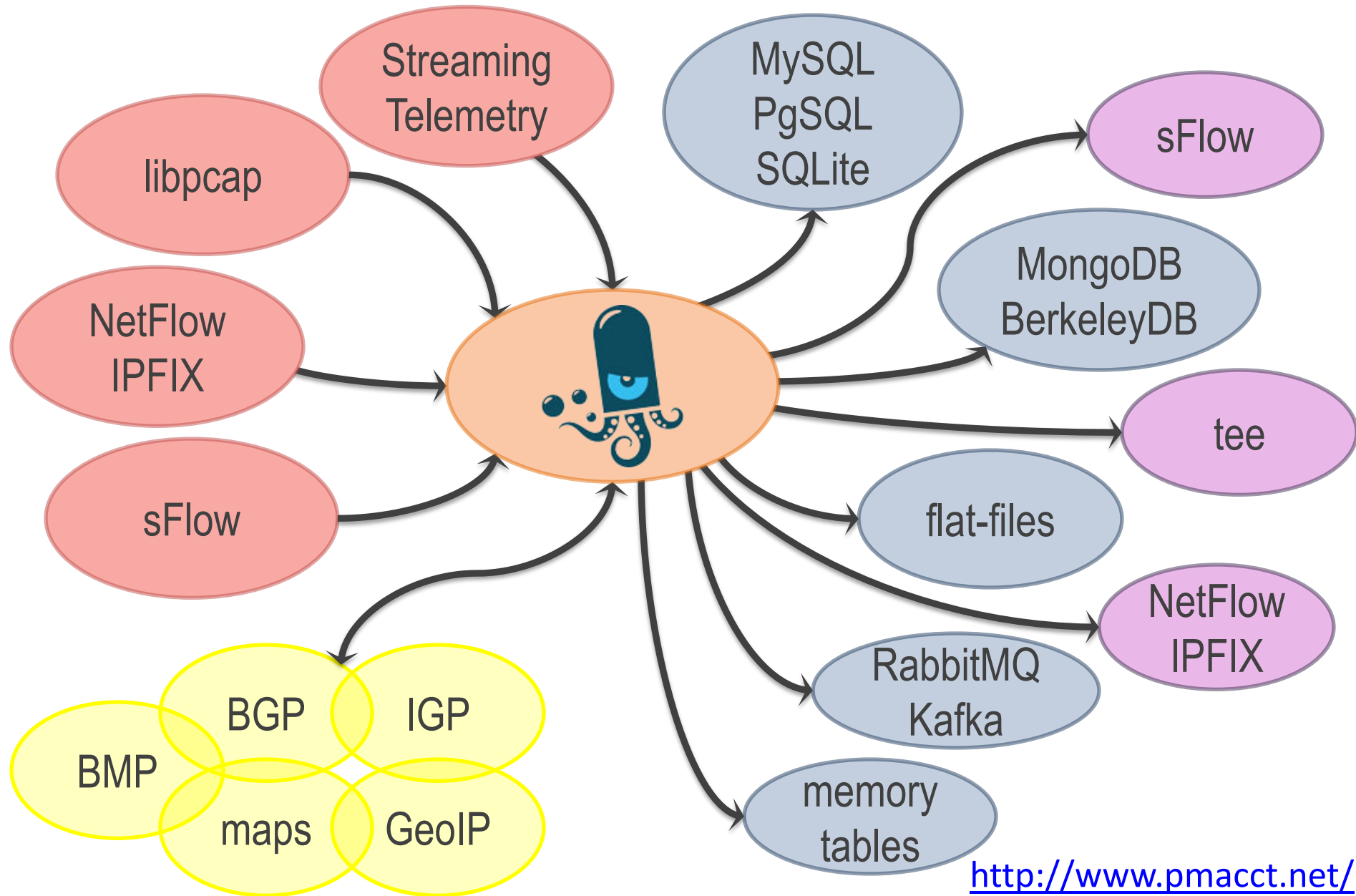
- Both drafts in their -01 version
- draft-ietf-grow-bmp-local-rib-00 -> -01:
  - Mainly text clarifications
  - Peer down VRF/Table name optional TLV [reduce state]
- draft-ietf-grow-bmp-adj-rib-out-00 -> -01:
  - Mainly text clarifications
  - Peer up Admin Label optional TLV [ie. to carry peer-group info]
- After -01 version some discussion happened on the GROW WG list. Further discussion is encouraged!



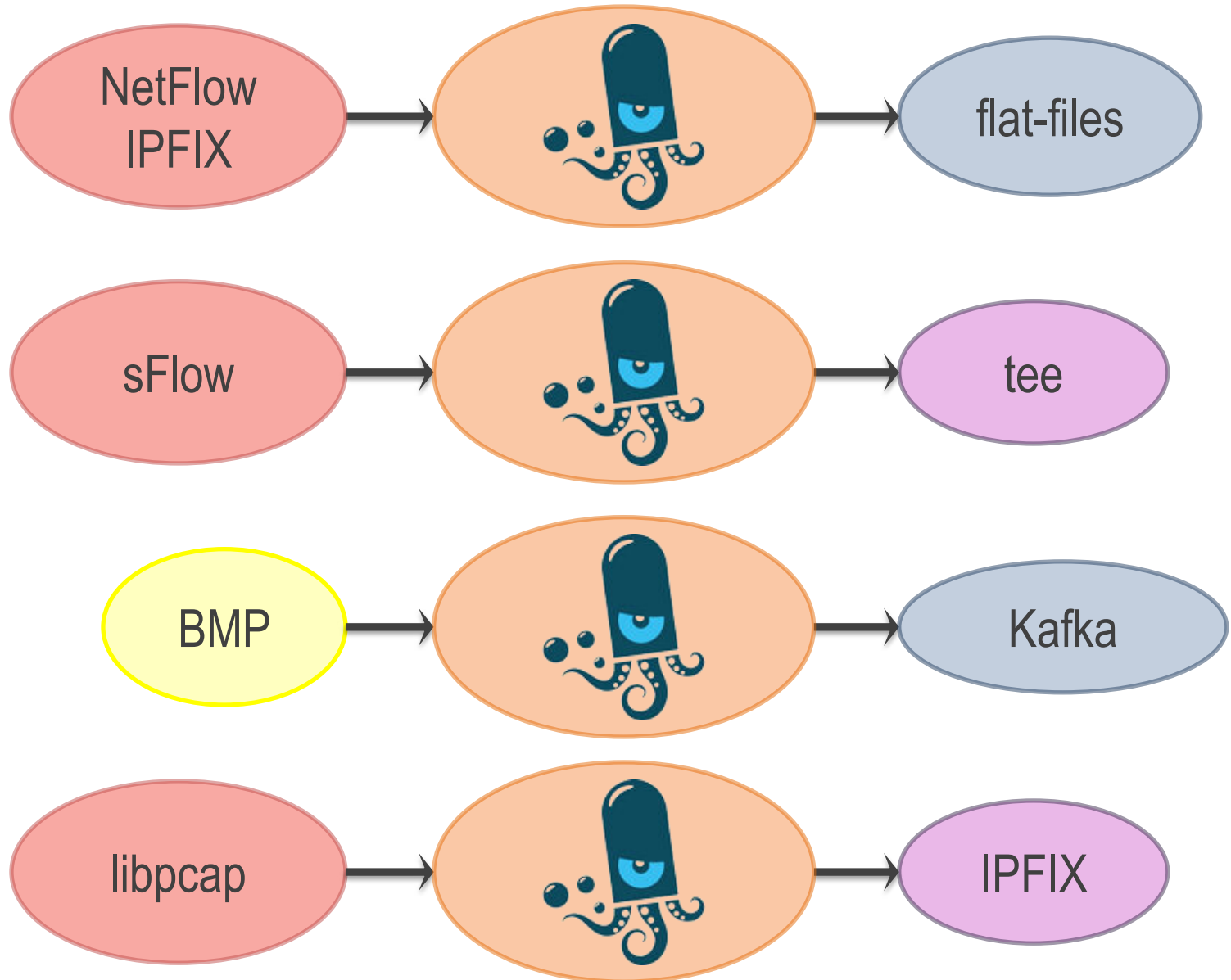
BMP data, including all being said so far, can be collected with pmacct  
(bear with me for the next few slides)



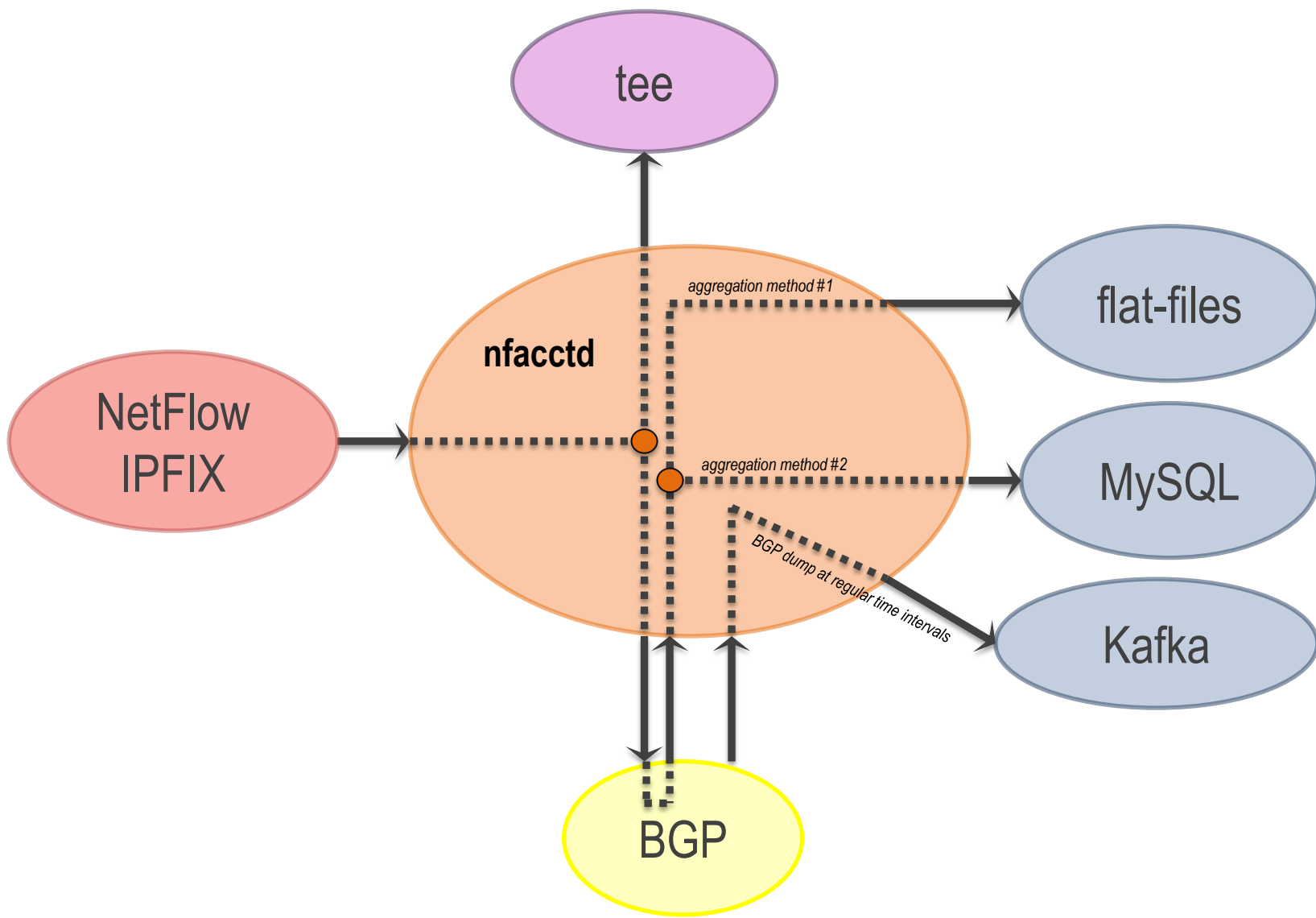
# pmacct is open-source, free, GPL'ed software



# pmacct: a few simple use-cases



# pmacct: a slightly more complex use-case



# The use-case for message brokers



kafka



RabbitMQ



elasticsearch



druid



InfluxDB



ClickHouse



Grafana kibana



Superset



# Latests on BGP monitoring

## Thanks! Questions?

Paolo Lucente

NTT Communications | pmacct