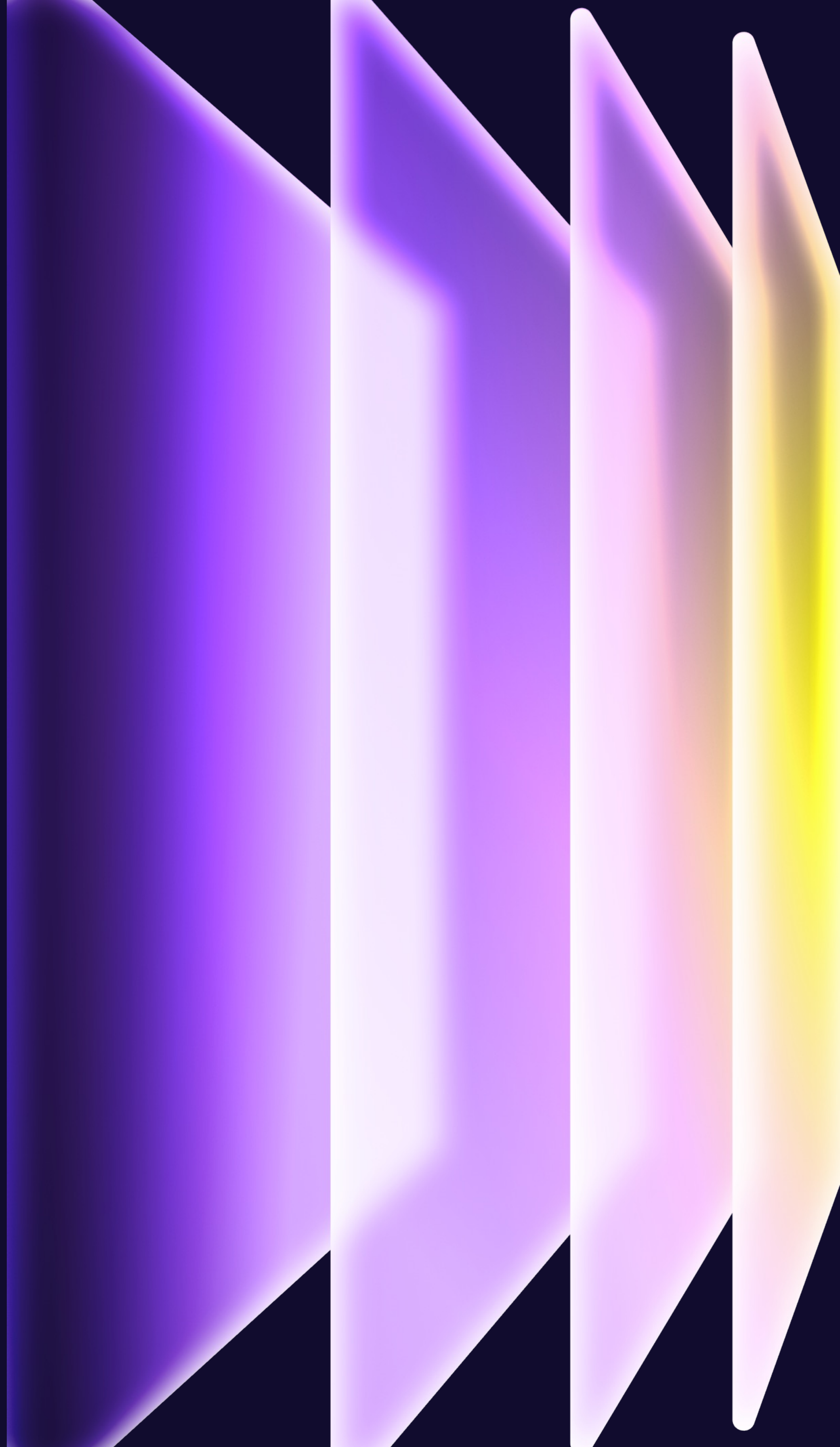
Infrastructure

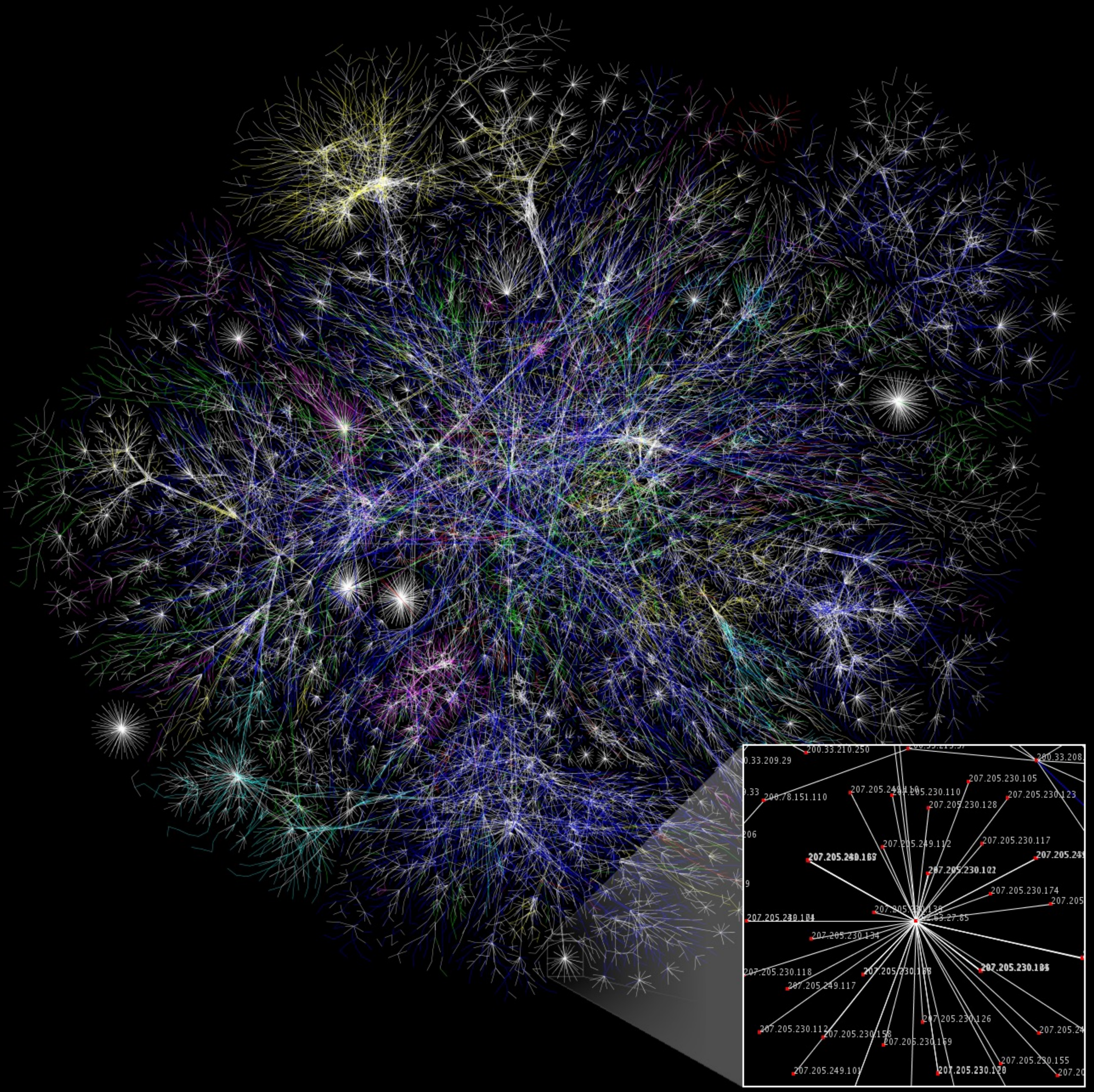
BGP & BMP Collections

Alexander Azimov, mitradir@yandex-team.ru



1. **Why do we need route collectors?**
2. What data is available?
3. How to process routing data?
4. Usage examples

Routing Data



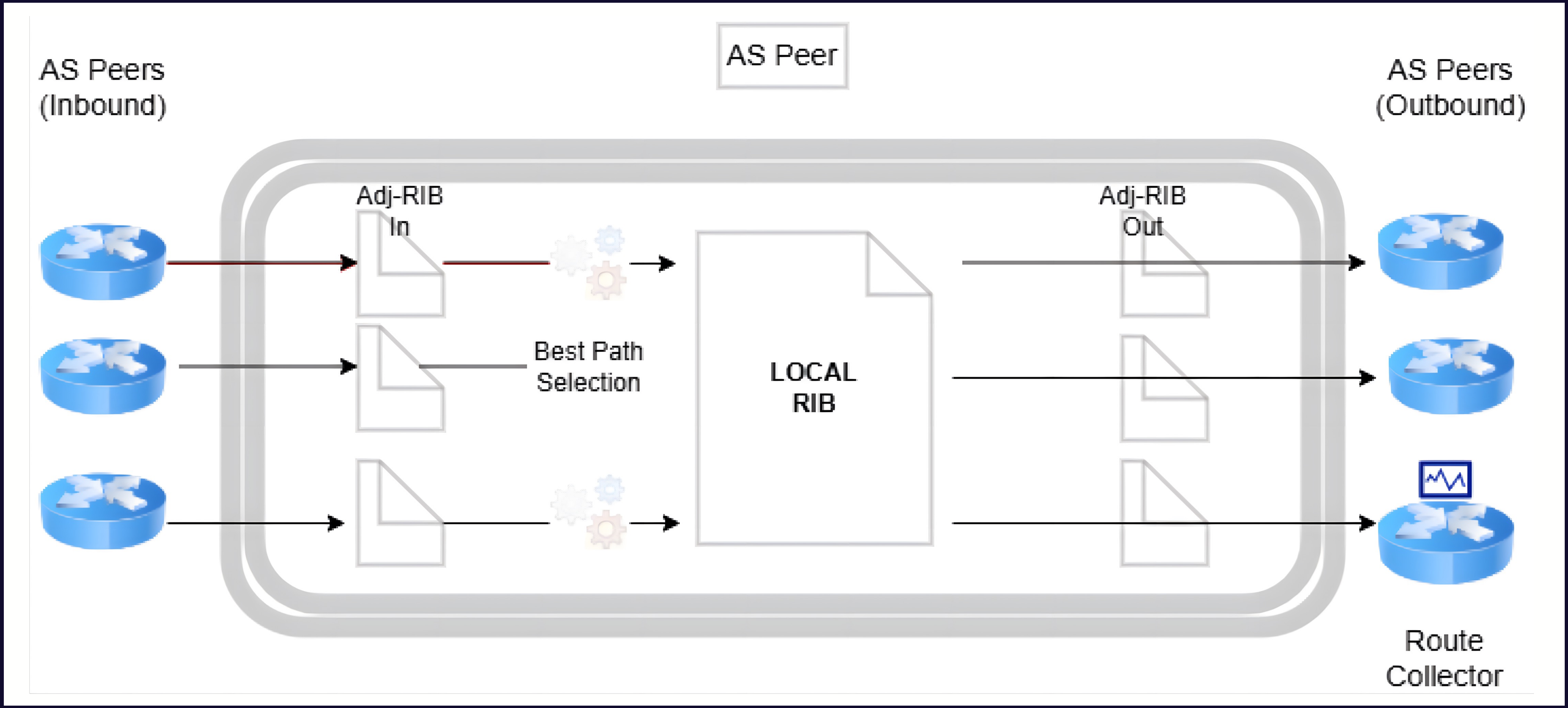
Why Do We Need Routing Data?

1. show route
2. Logs
3. IP Lookup (GEO)
4. TE / Capacity planning
5. Injectors
6. Monitoring

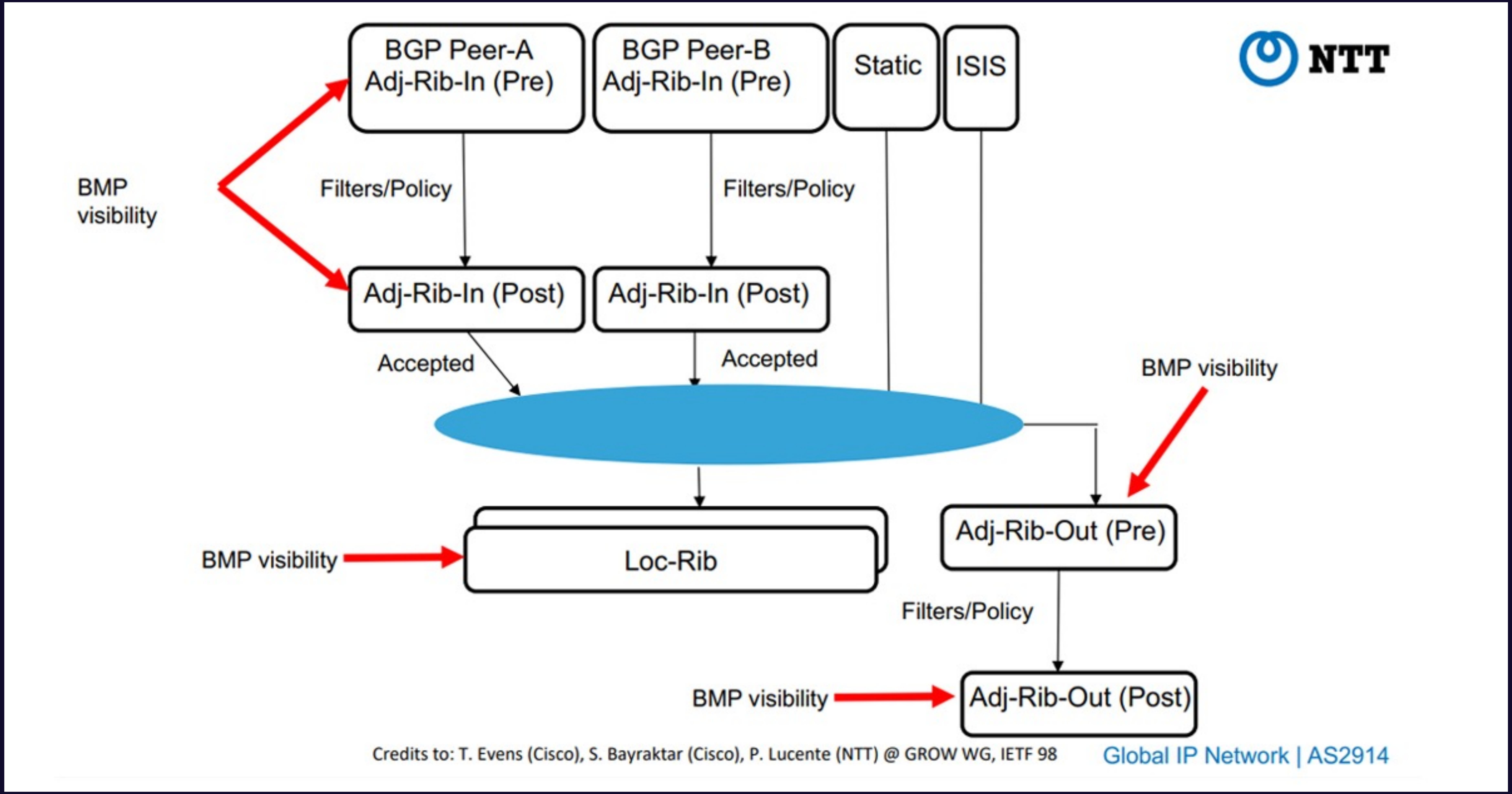
Realtime

1. **Why do we need route collectors?**
2. **What data is available?**
3. How to process routing data?
4. Usage examples.

Classic BGP Collector



BMP Collector



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

Rib-Pre

Usually

Rib-Post

Often

Loc-Rib

Sometimes

Loc-Out

Crap!

MAYBE
BOTH
makeameme.org

BGP

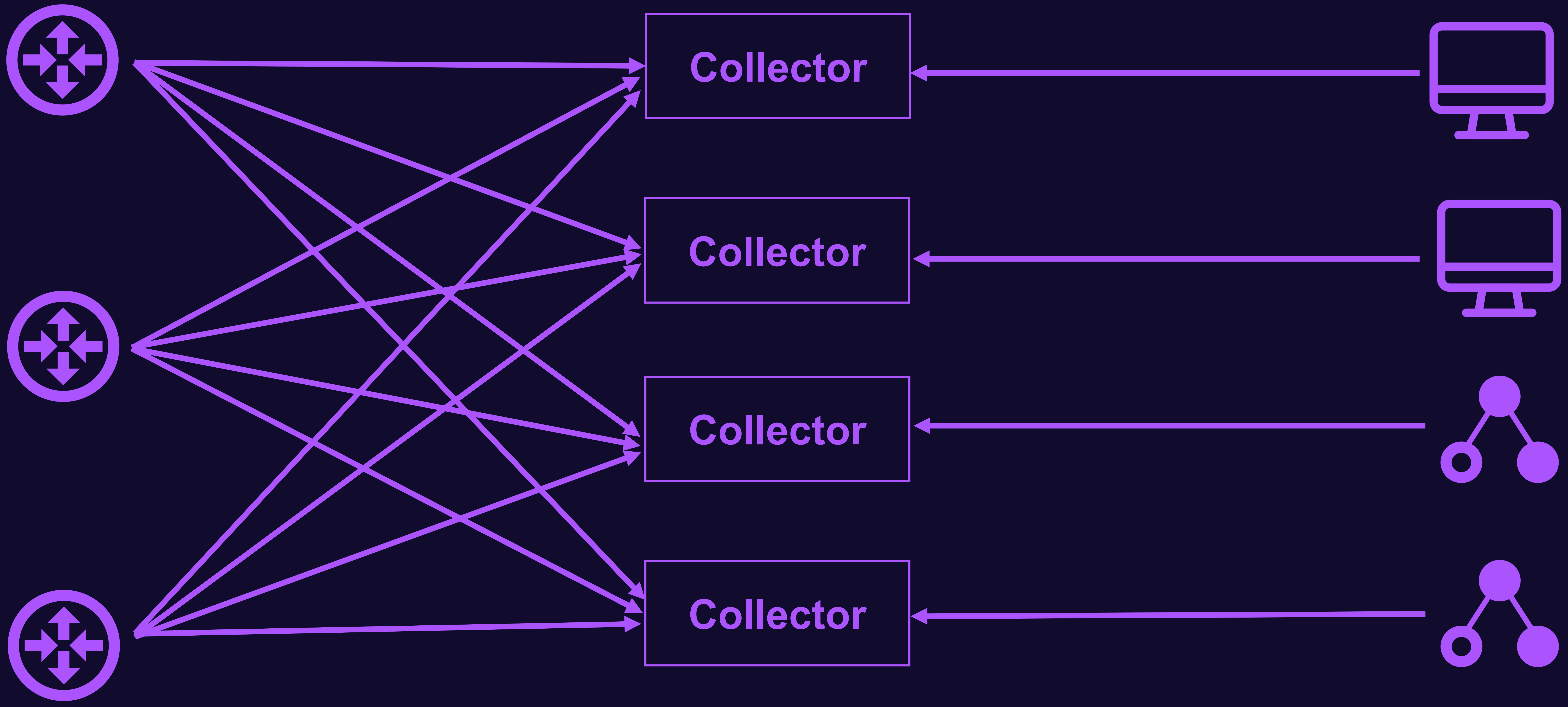
- FRR
- BIRD
- GoBGP
- bgpdump
- ExaBGP
- PMACCT

BMP

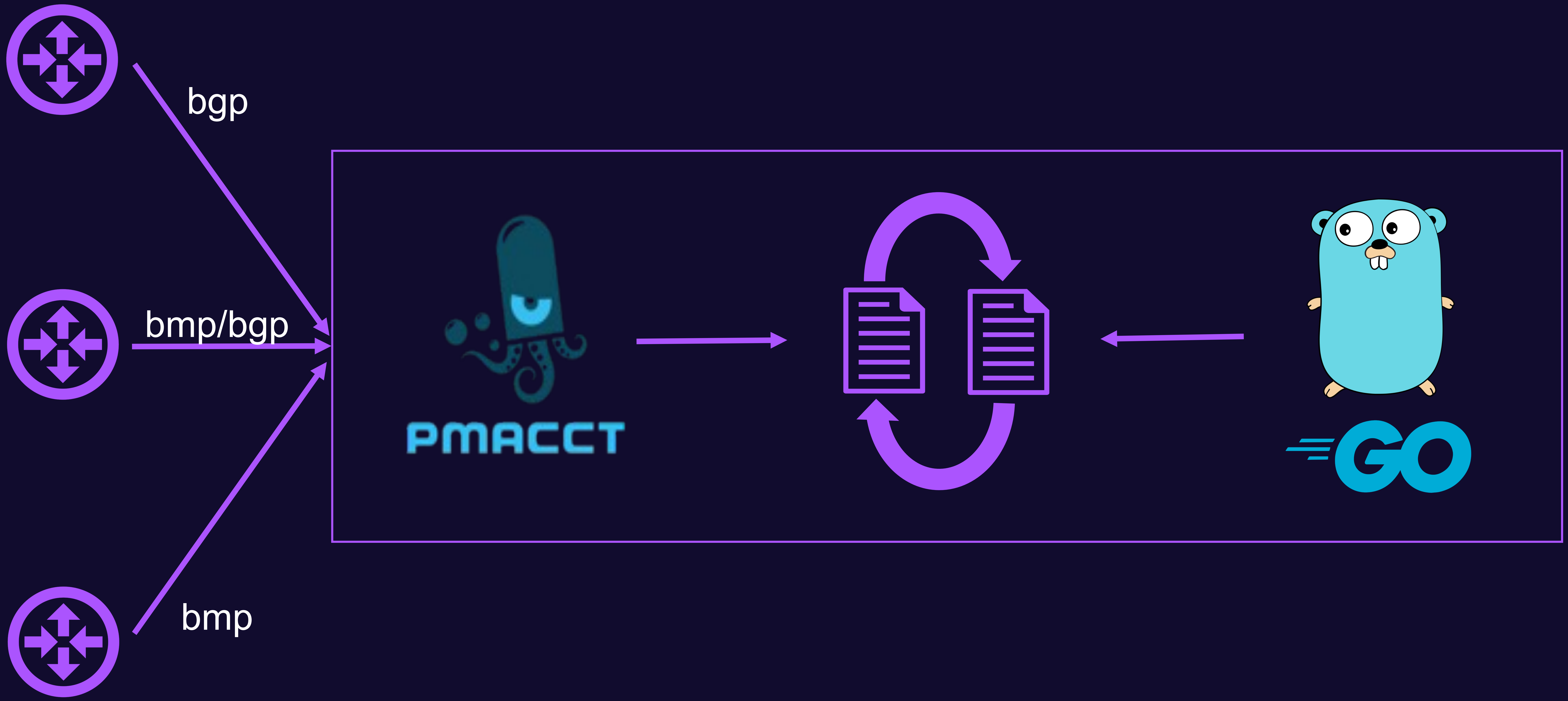
- bbmp2kafka
- Gobmp
- YABMP
- OpenBMP
- PMACCT

1. Why do we need route collectors?
2. What data is available?
3. **How to collect routing data?**
4. Usage examples

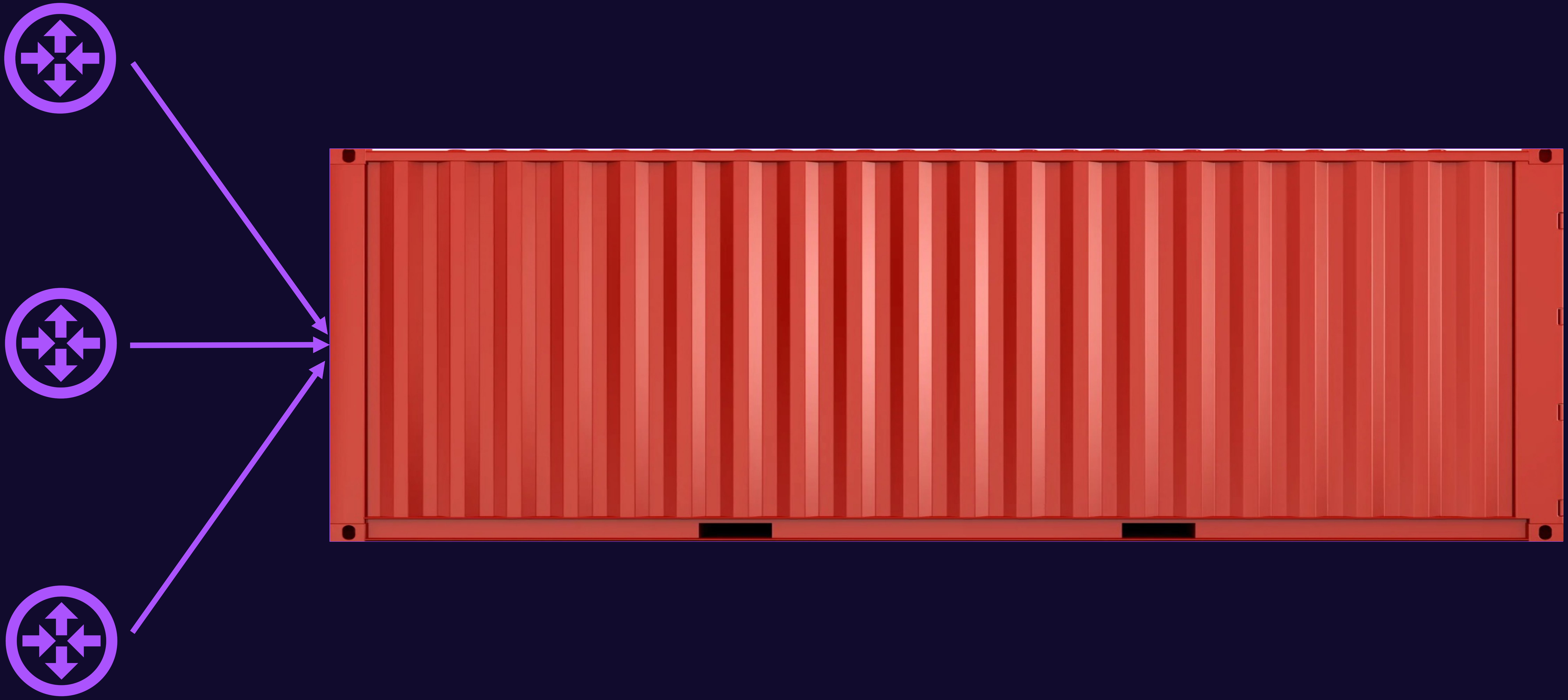
How to collect routing data?



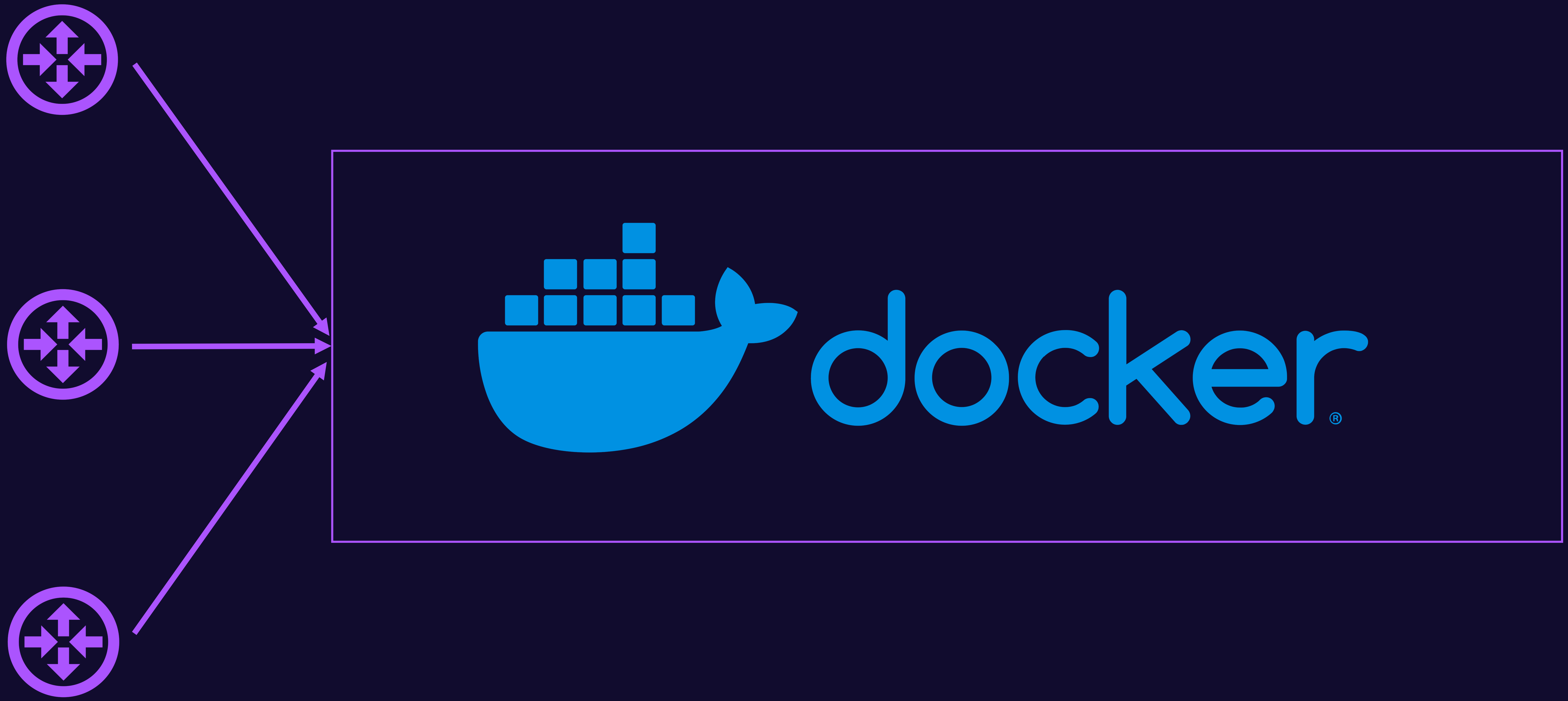
Collector



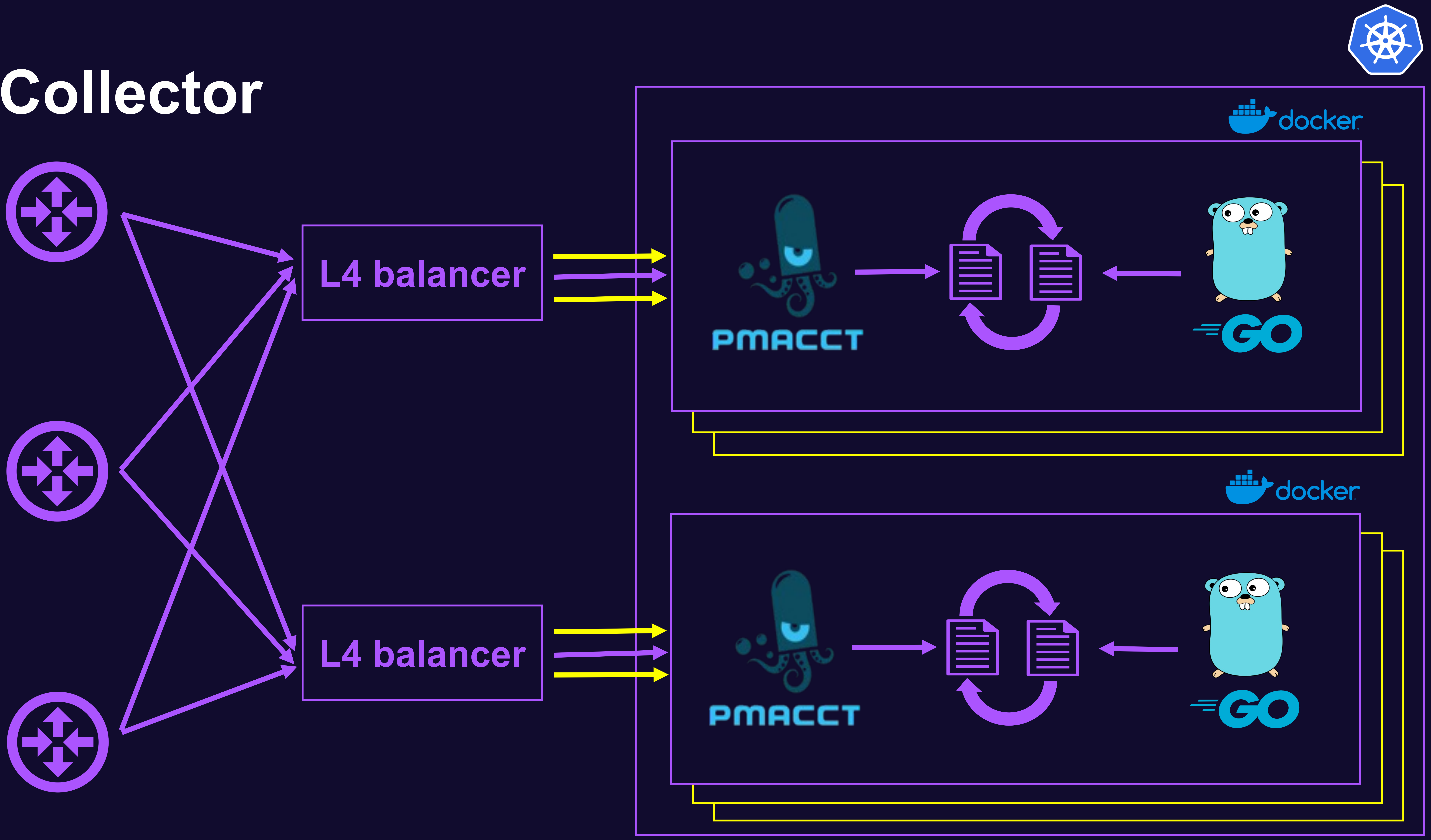
Collector



Collector



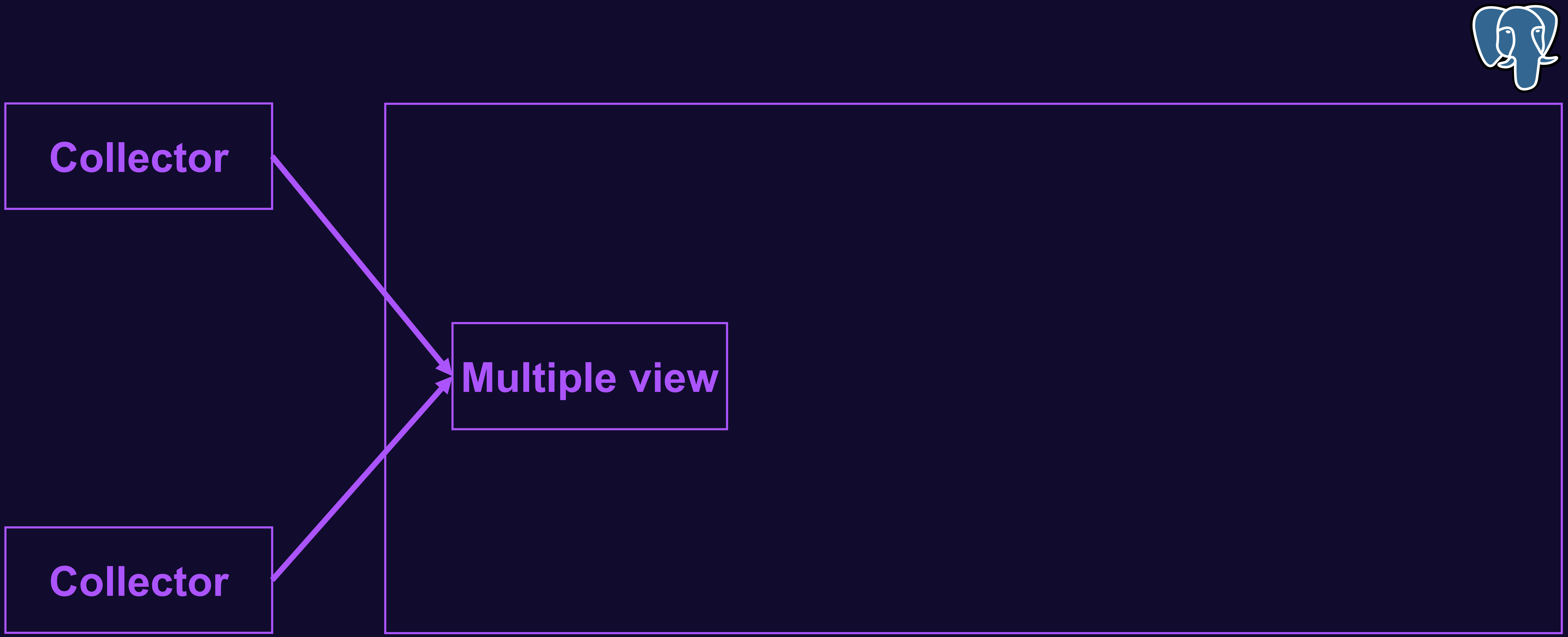
Collector



Storage requirements

1. Consistency
2. Distribution
3. Performance

Storage



Collector

Collector

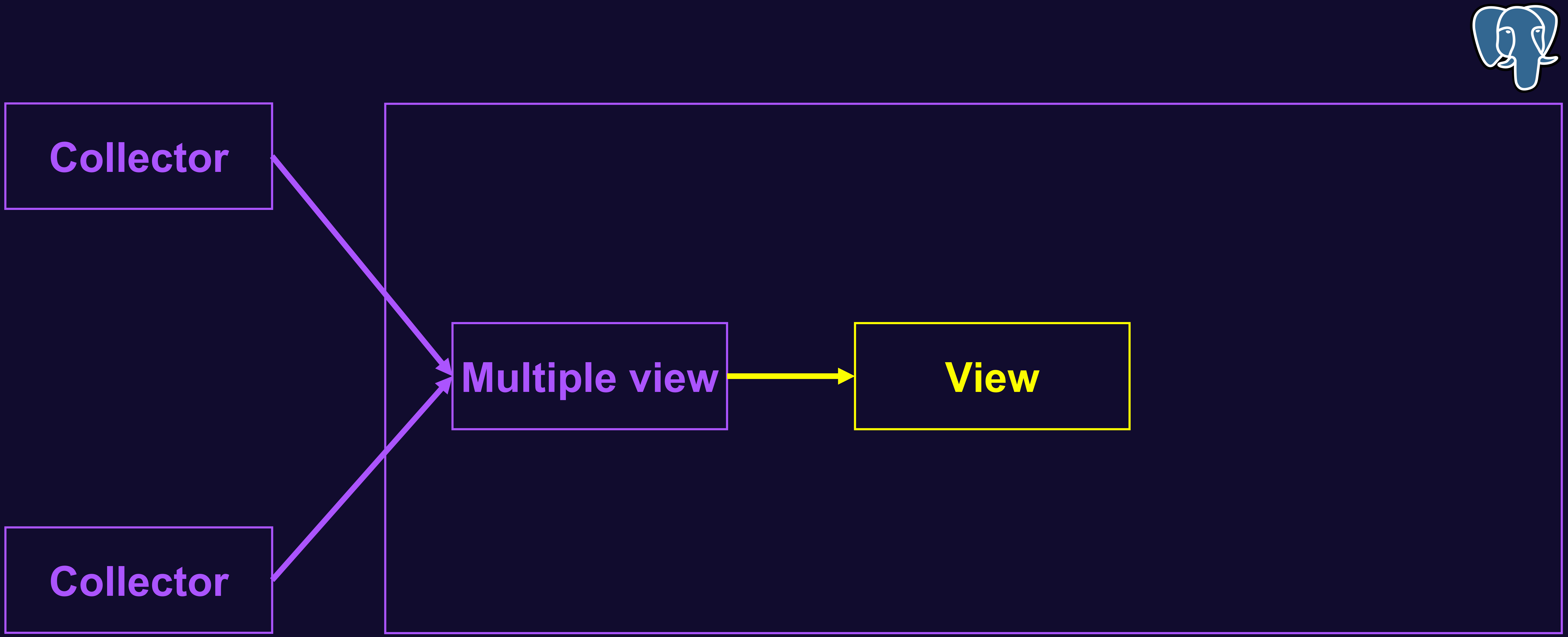
Multiple view

Deduplication

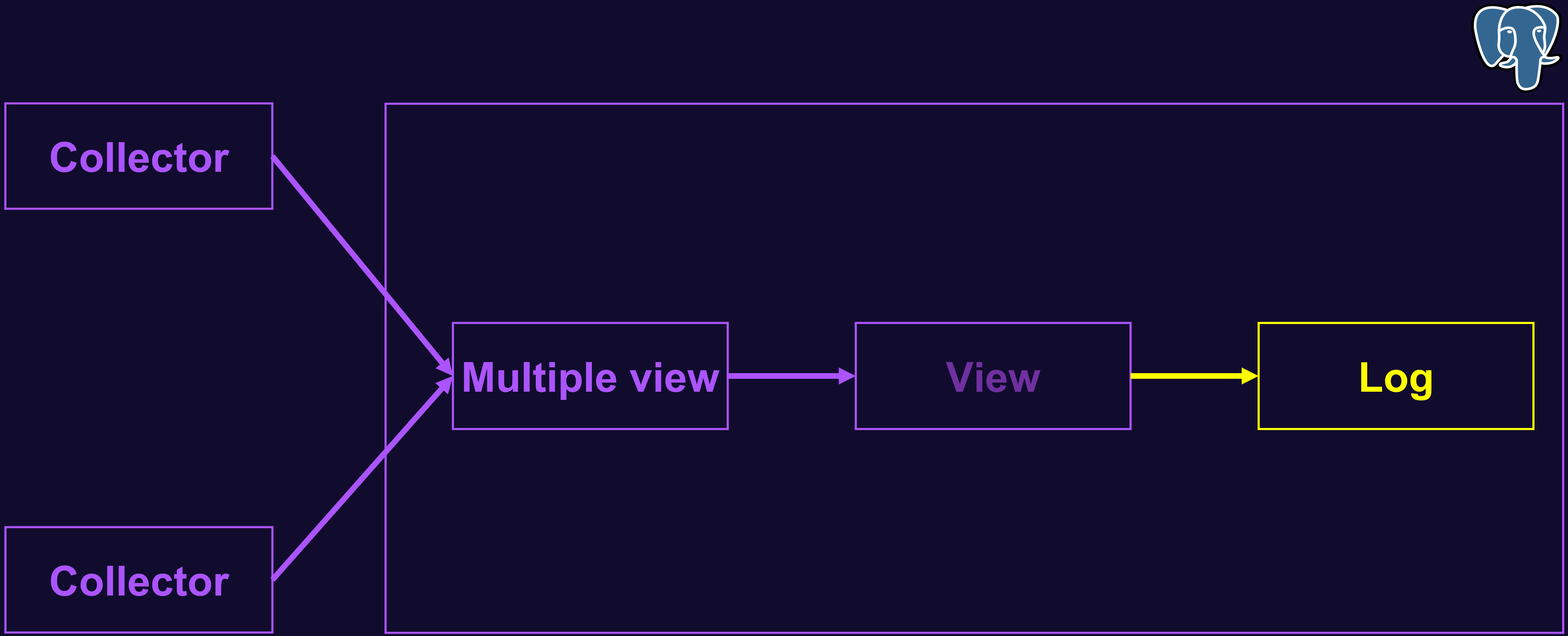
BGP: Ordered by best path selection

BMP: Ordered by timestamp arrival

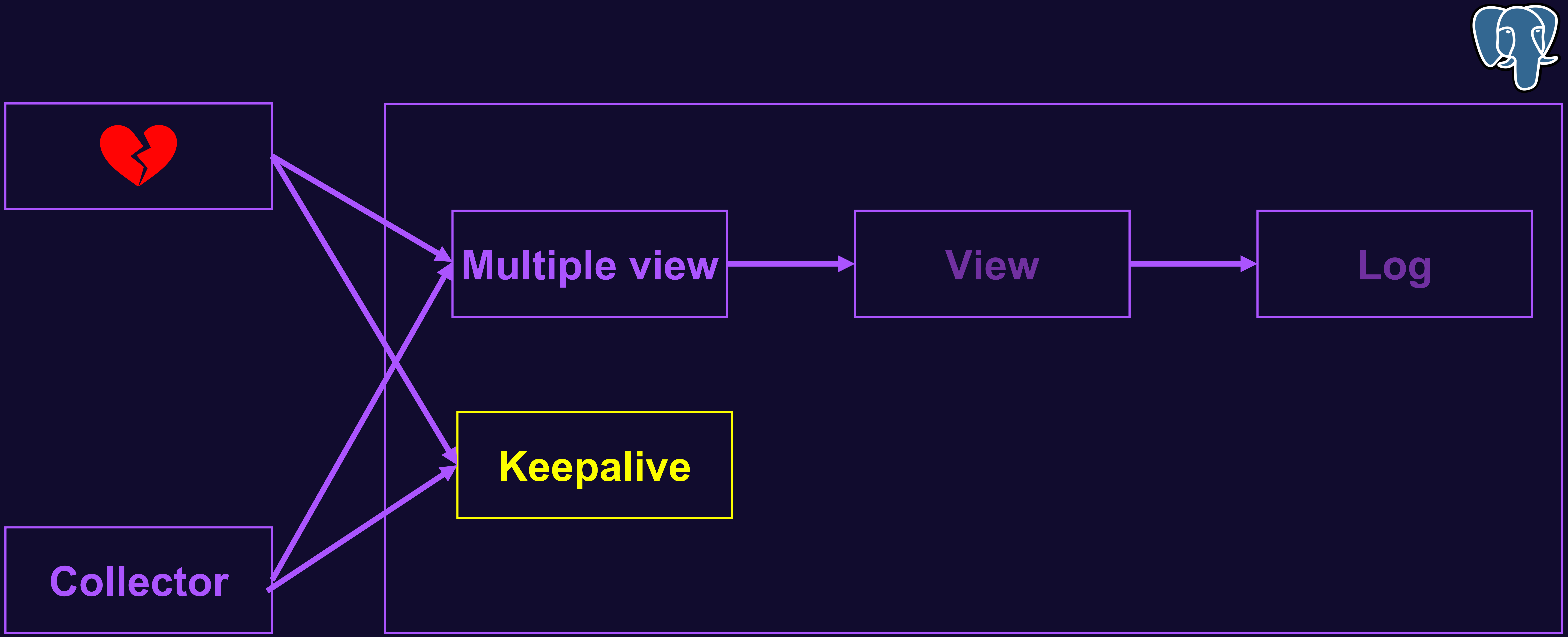
Storage



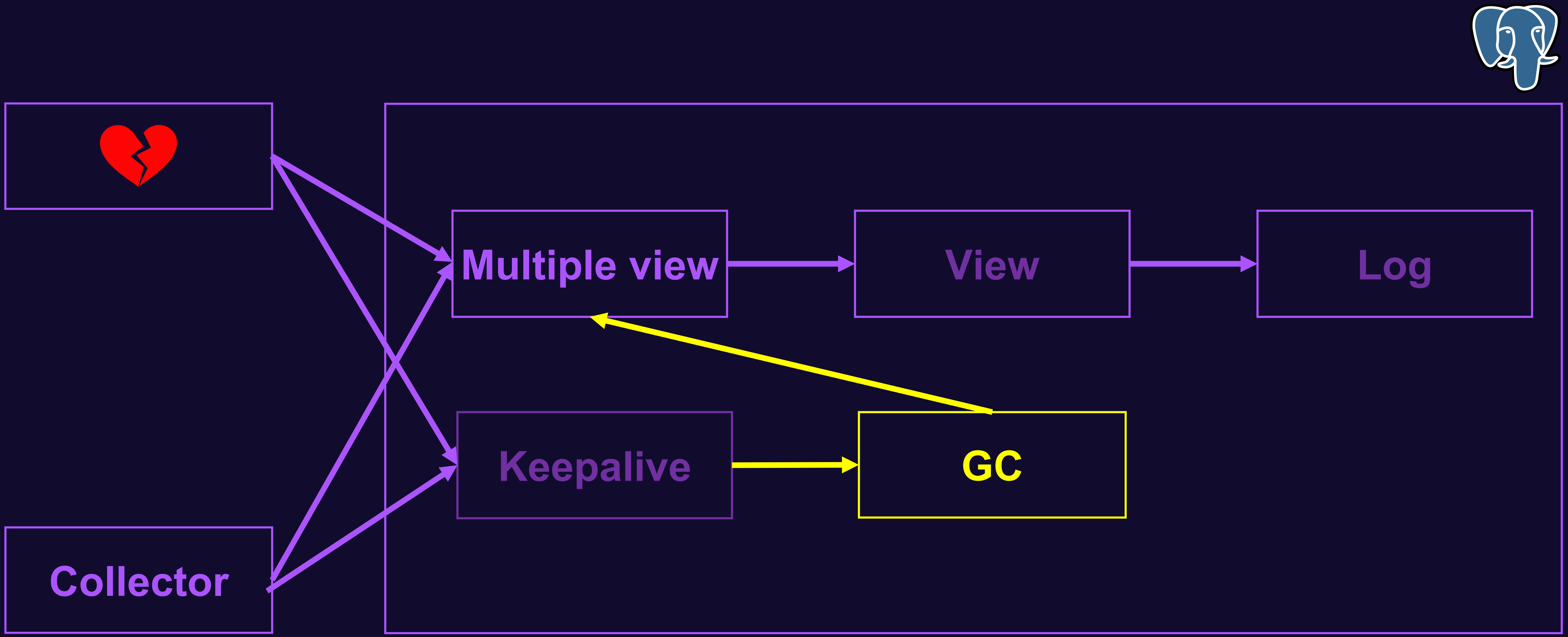
Storage



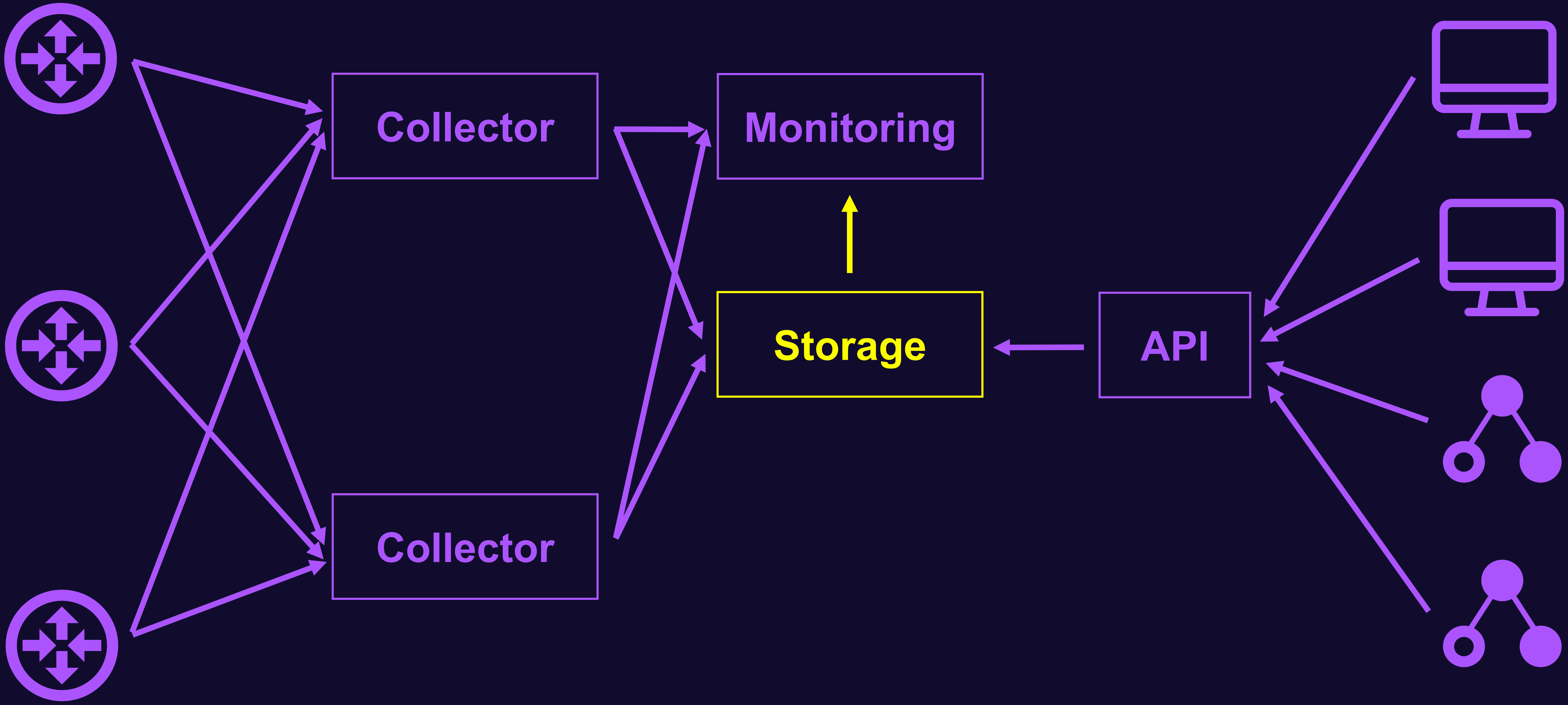
Storage



Storage



Storage



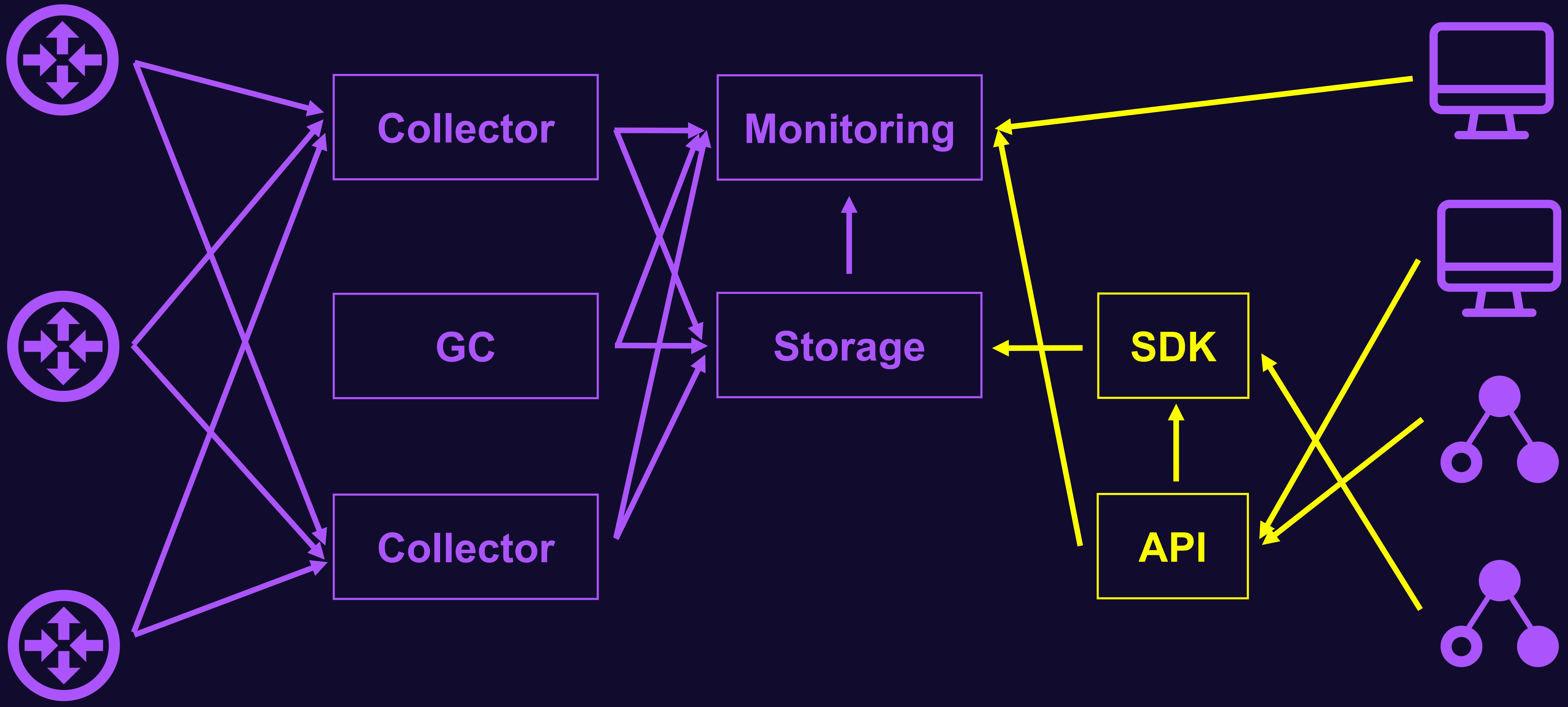
API

- Full/best view at any moment
- IP Lookup

SDK

- Full/best view at any moment
- IP Lookup
- Full/best view and updates
- Client
- Performance

Architecture



Collected routes

Source	BGP	BMP
Borders	✓	✓
CDN	✓	
RR	✓	
DC PE		✓

1. Why do we need route collectors?
2. What data is available?
3. How to collect routing data?
4. Usage examples

Why Do We Need Routing Data?

1. show route
2. Logs
3. IP Lookup (GEO)
4. TE / Capacity planning
5. Injectors
6. Monitoring

Realtime

Routing Incidents

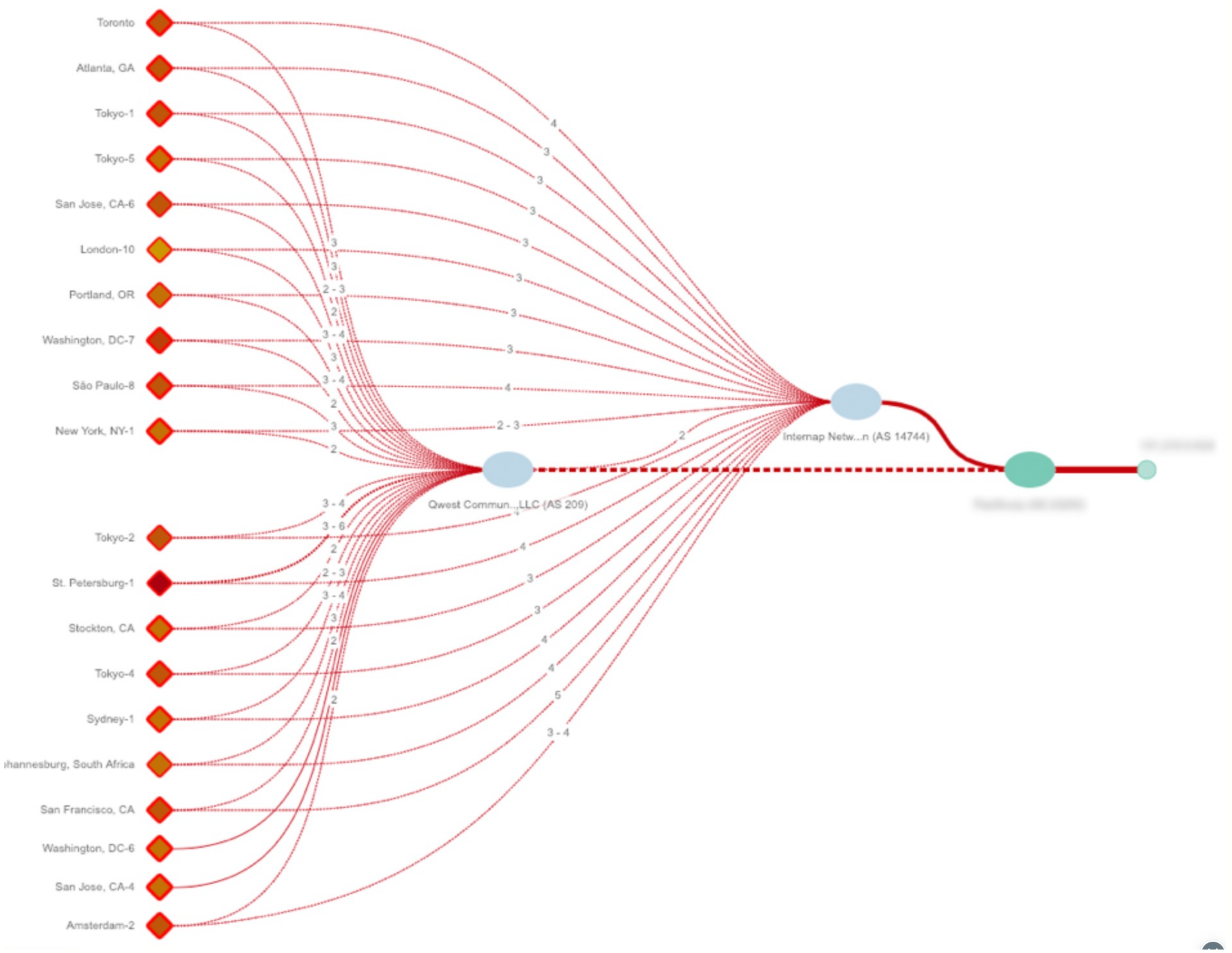
BGP Hijacks

When an illegitimate takeover of the address space is advertised via BGP

BGP Route Leaks

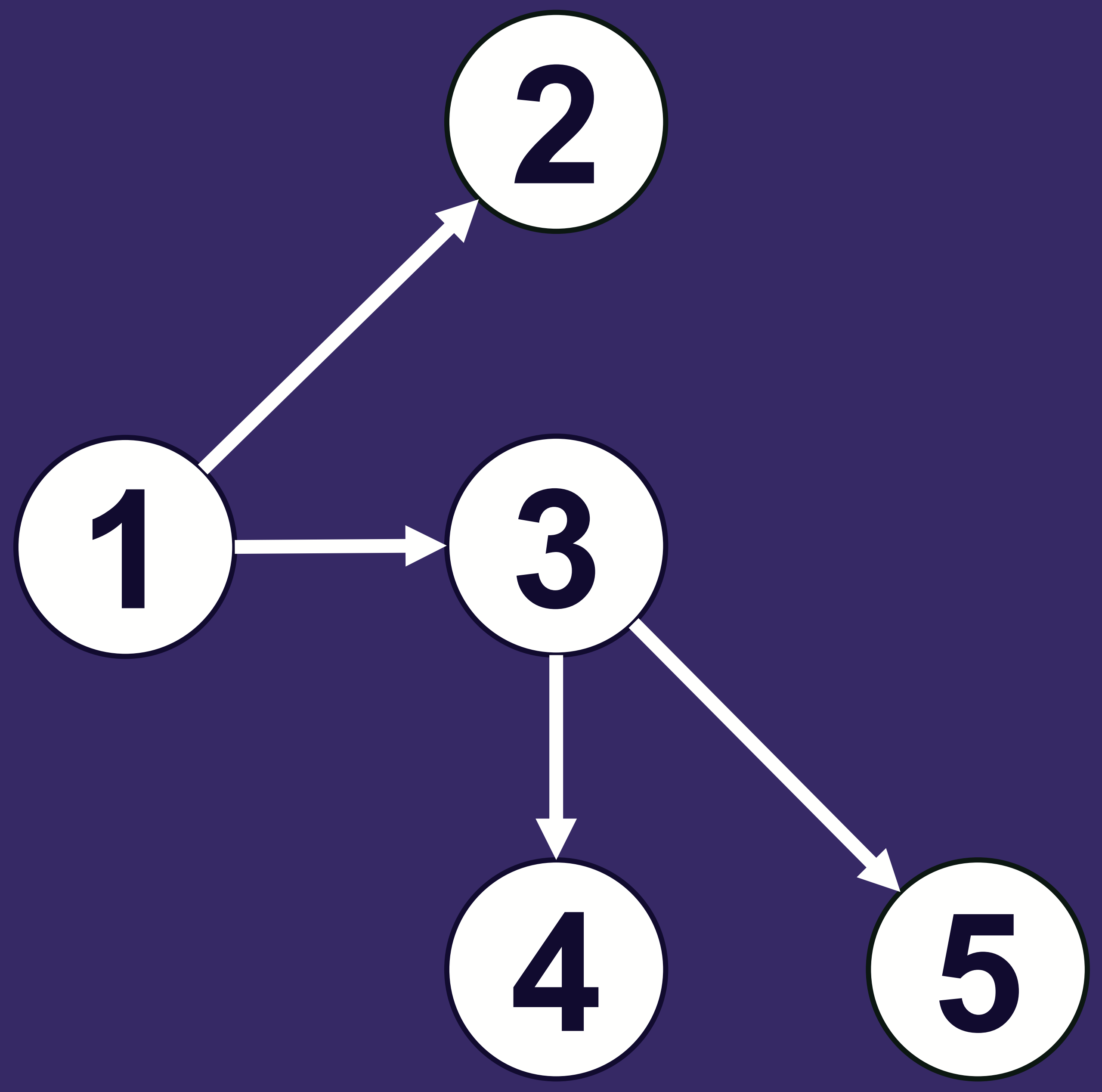
When a route is received from one provider or peer and is advertised to another provider or peer

Classic BGP Monitoring

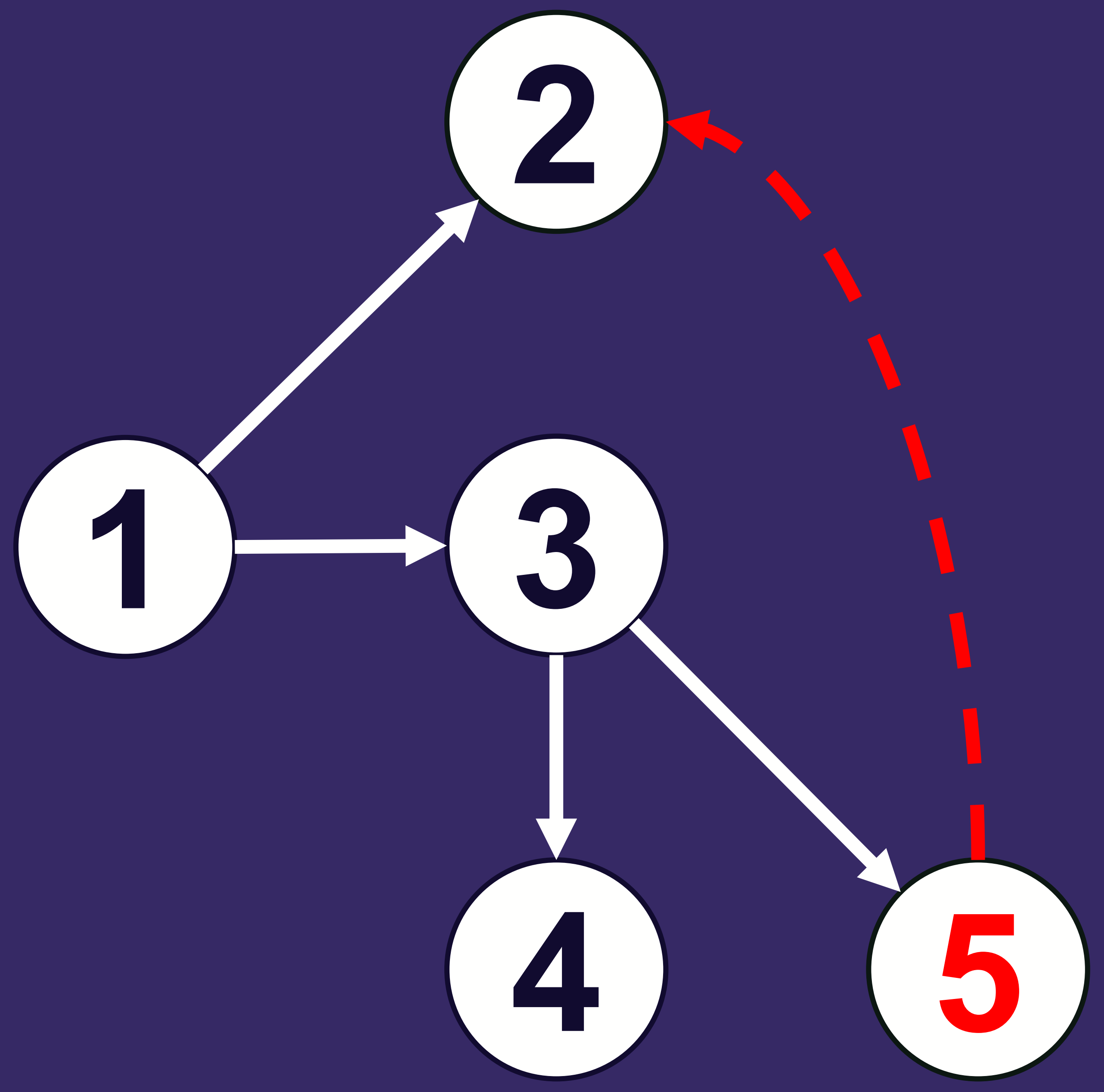


Temet Nosce

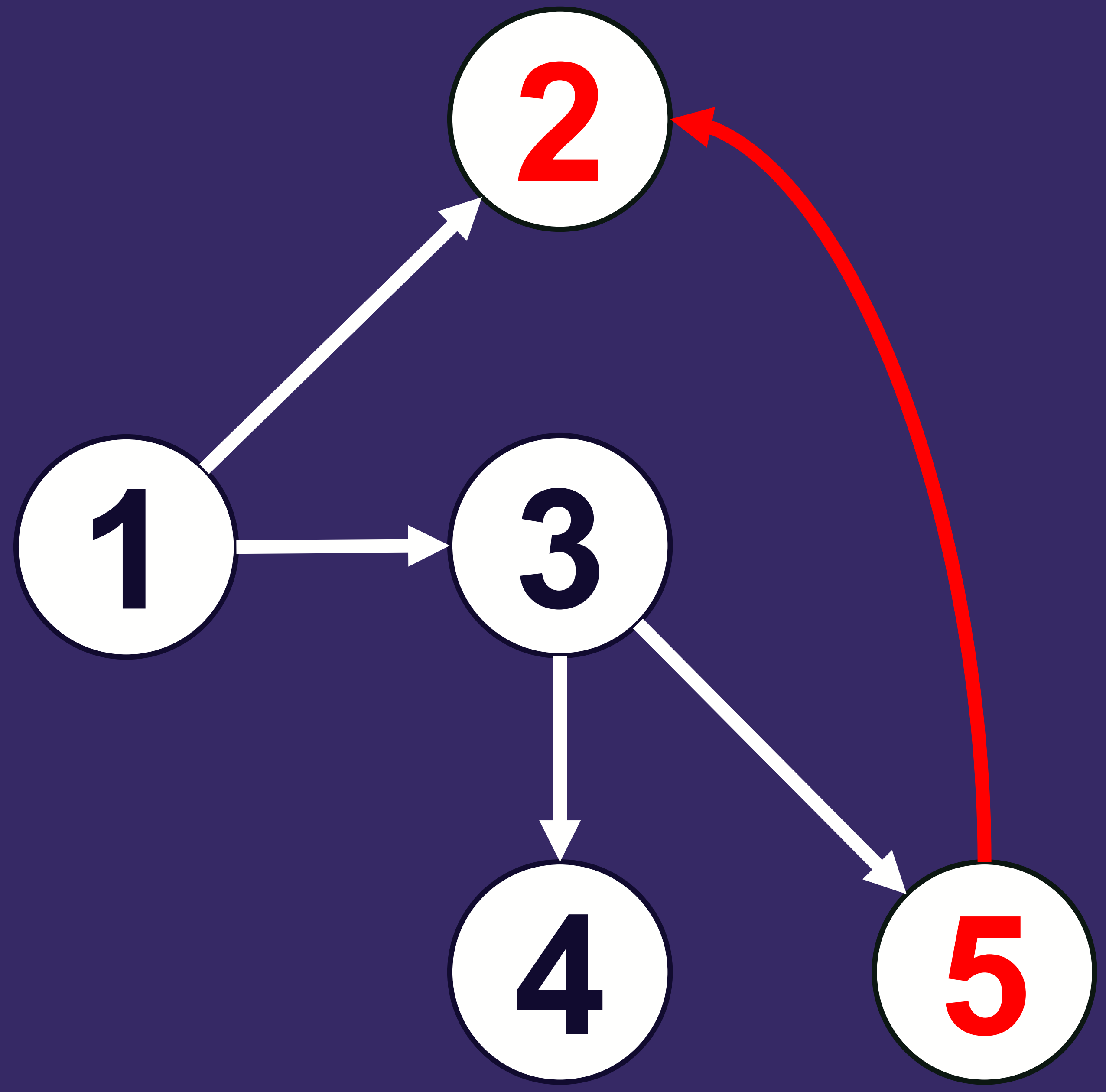
No Leaks – Good Leaks



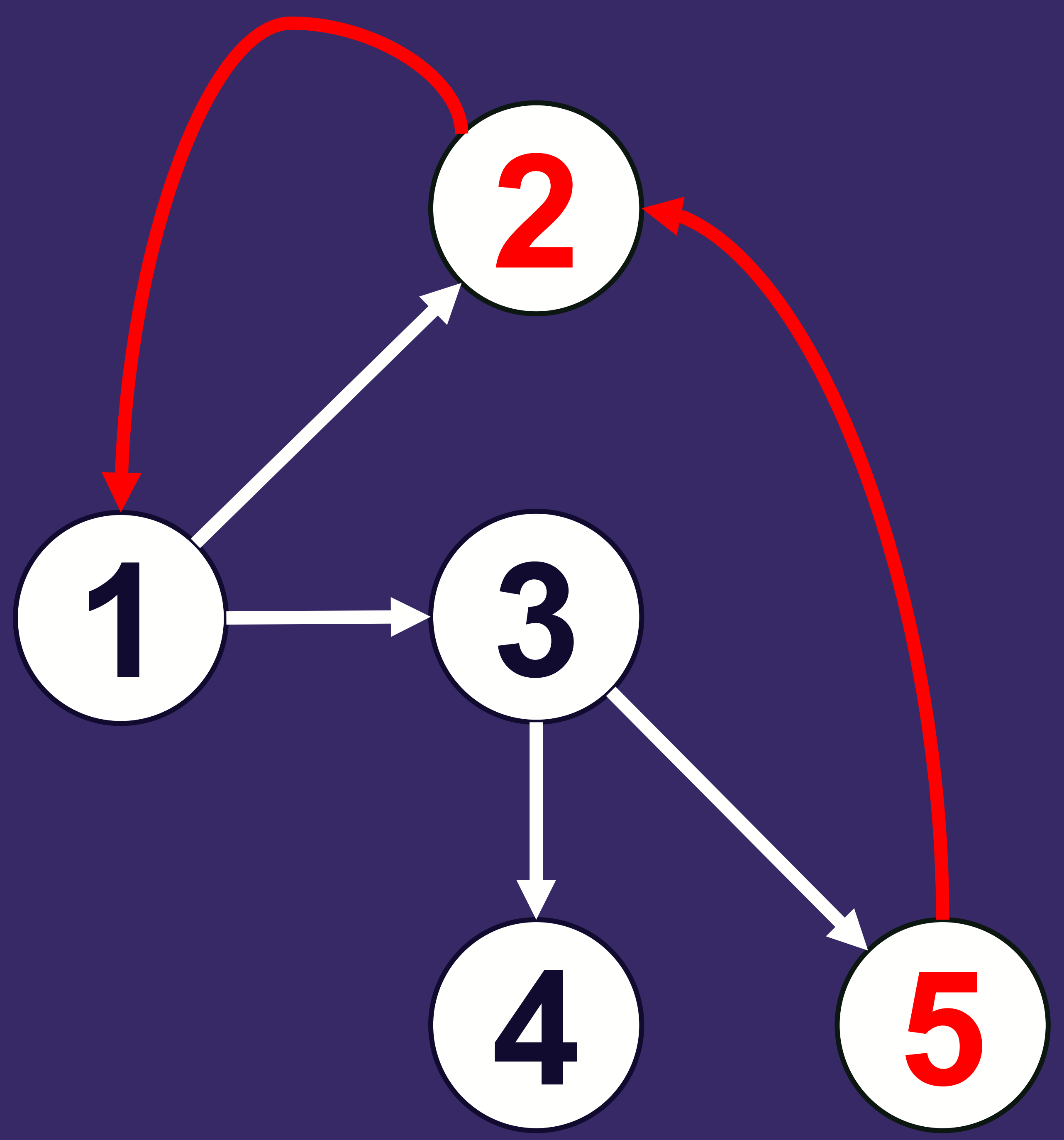
Not Propagated Leaks – Good Leaks

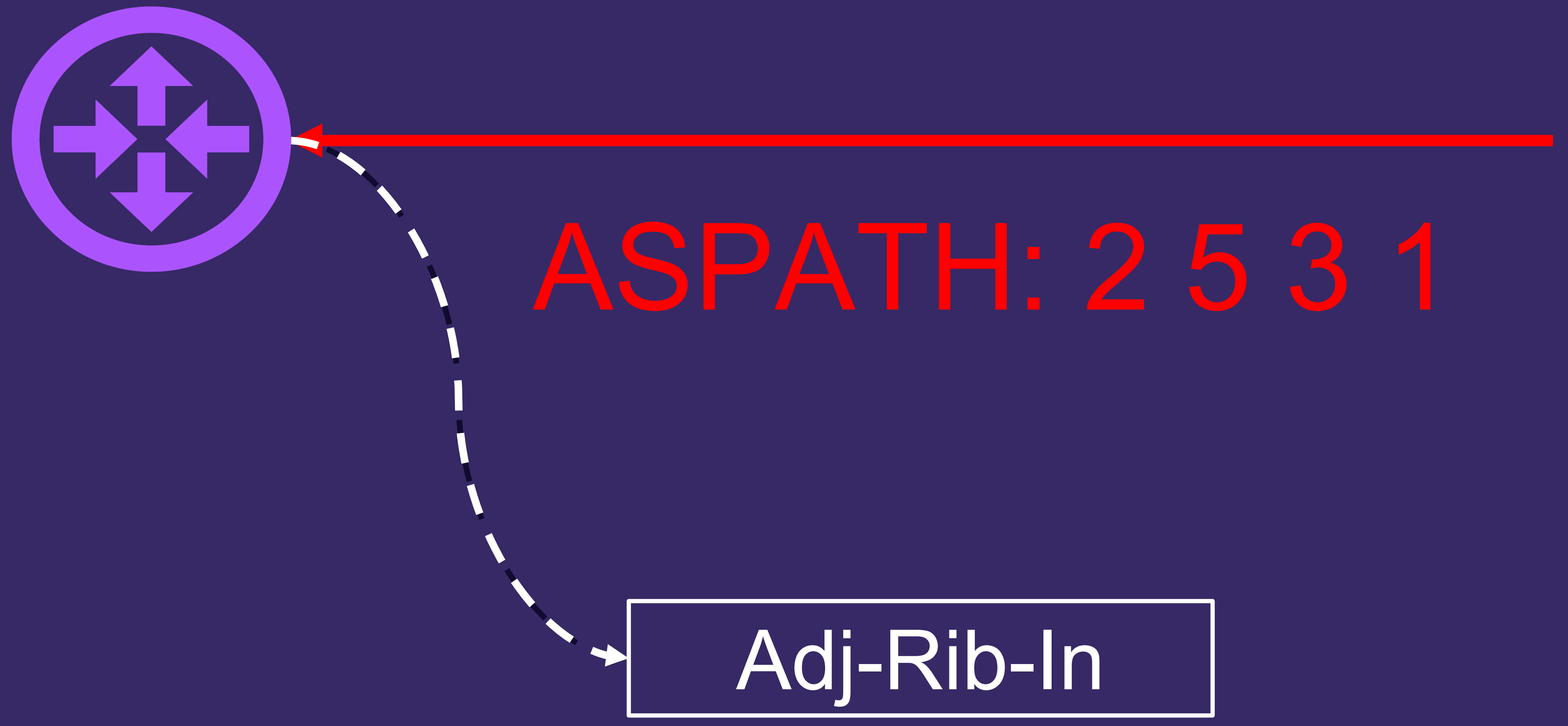


Propagating Leaks – Detection is Needed



Y-Detector: Key Idea

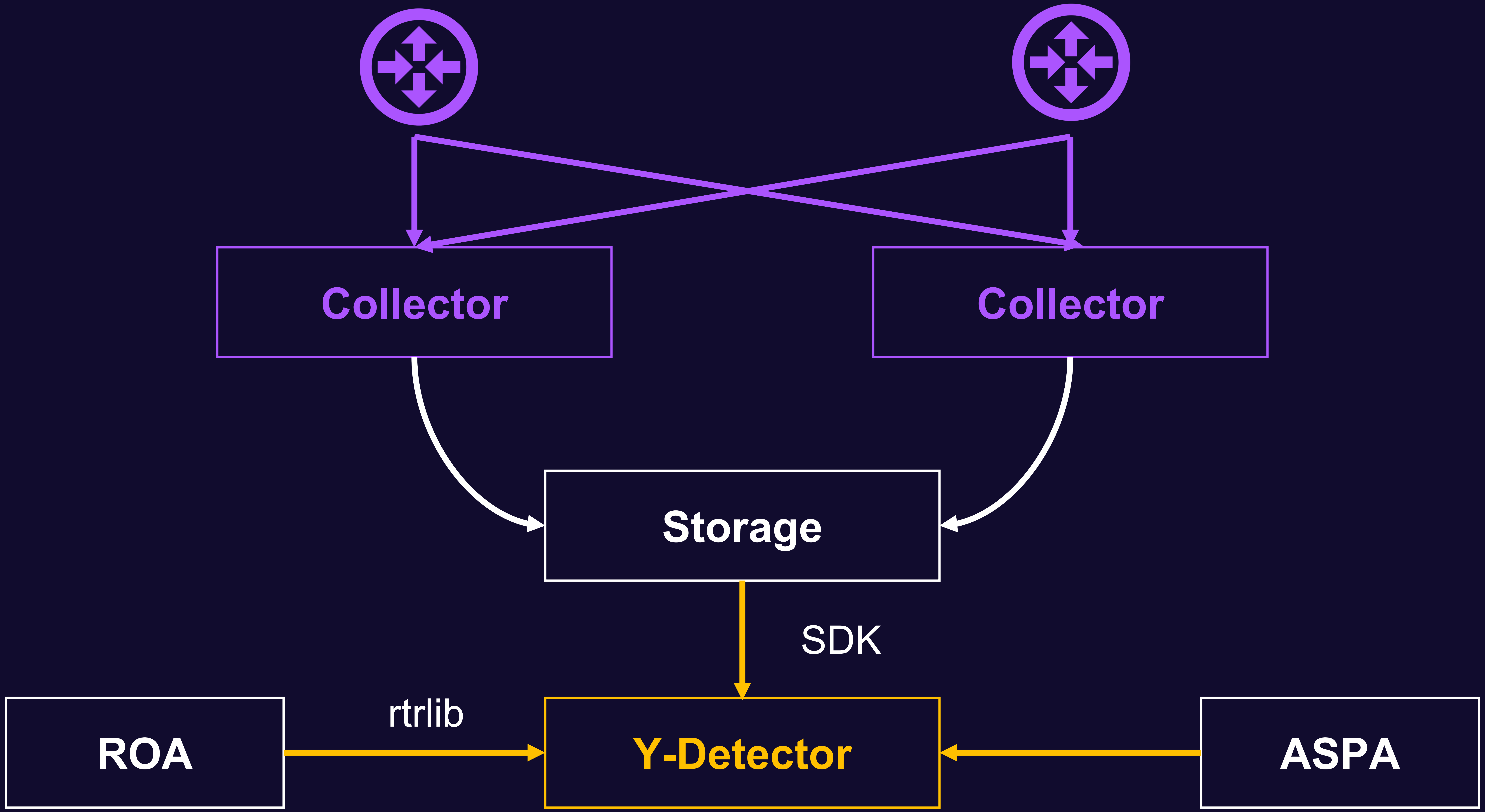


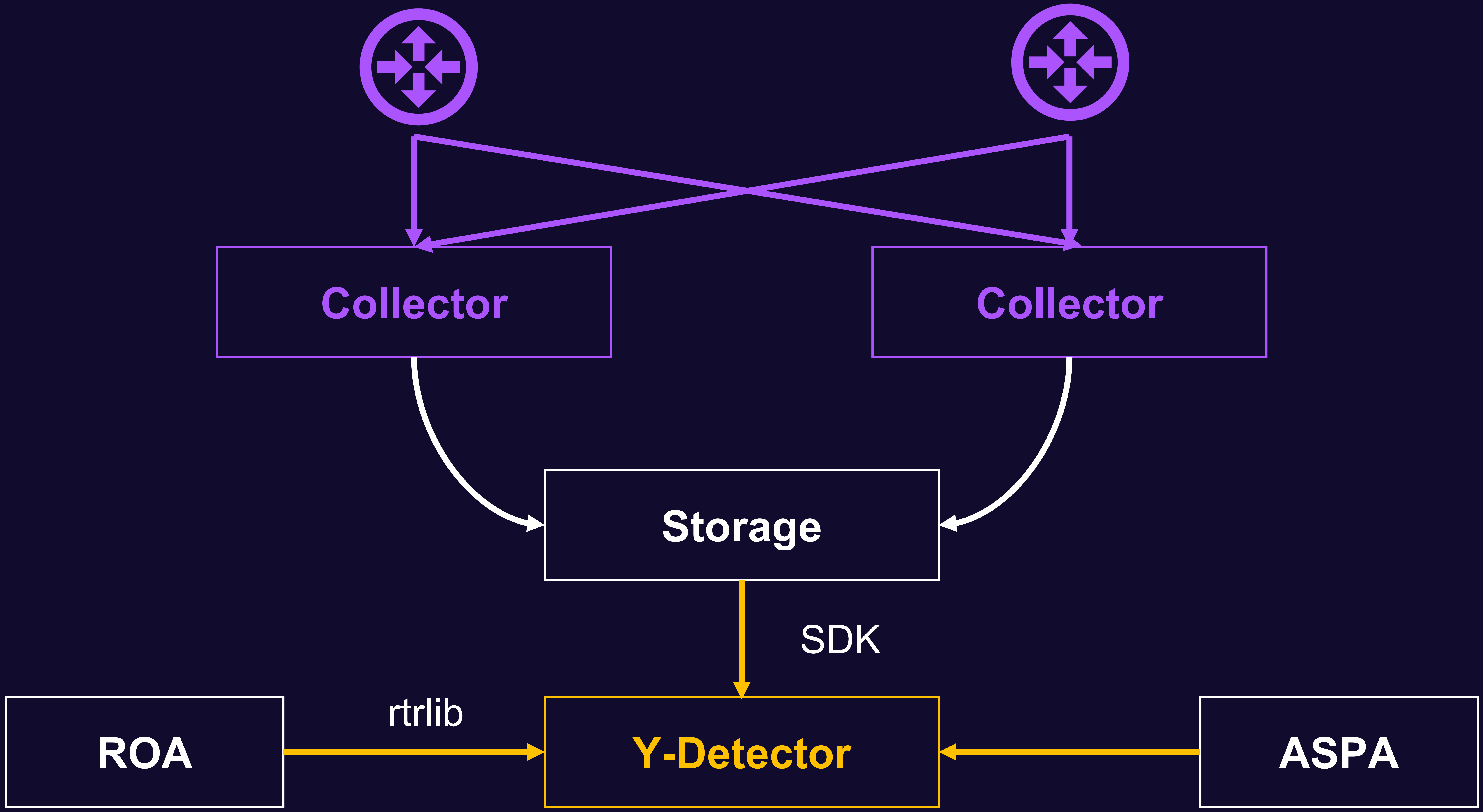


ASPATH: 2 5 3 1

Adj-Rib-In

If your neighbor accepts leaked/hijacked prefix, it will send it to you.
It will send your own address space too!


Collector
Collector
Storage
SDK
rtrlib
ROA
Y-Detector
ASPA



Wait, what is ASPA?

Autonomous System Provider Authorization

[draft-ietf-sidrops-aspa-verification]()

[draft-ietf-sidrops-aspa-profile]()

[draft-ietf-sidrops-8210bis]()

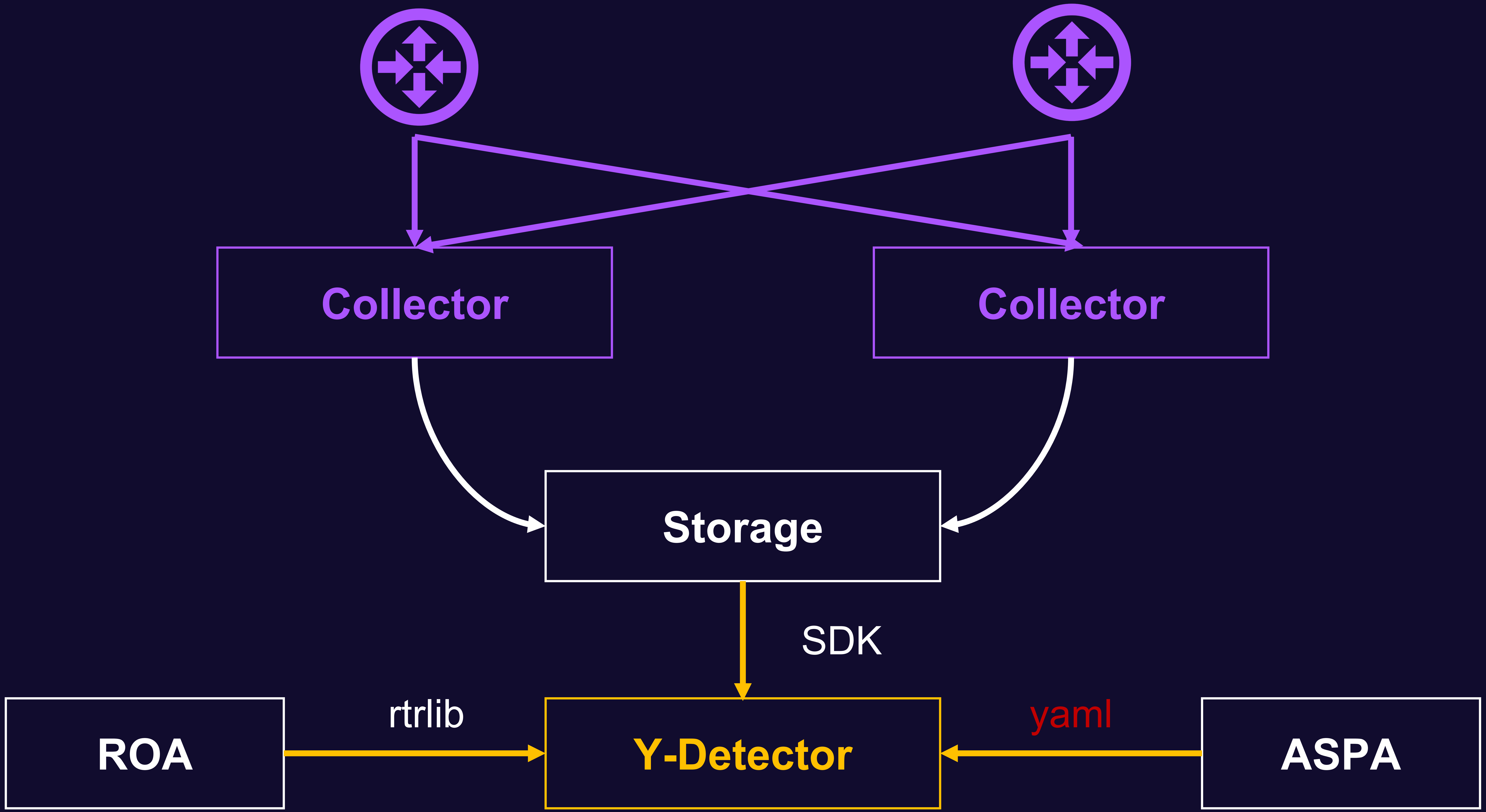
ASPA

- customer – signer
- providers – authorized to send routes to upper providers or peers
- AFI agnostic

How Many ASPAs Do You Need?

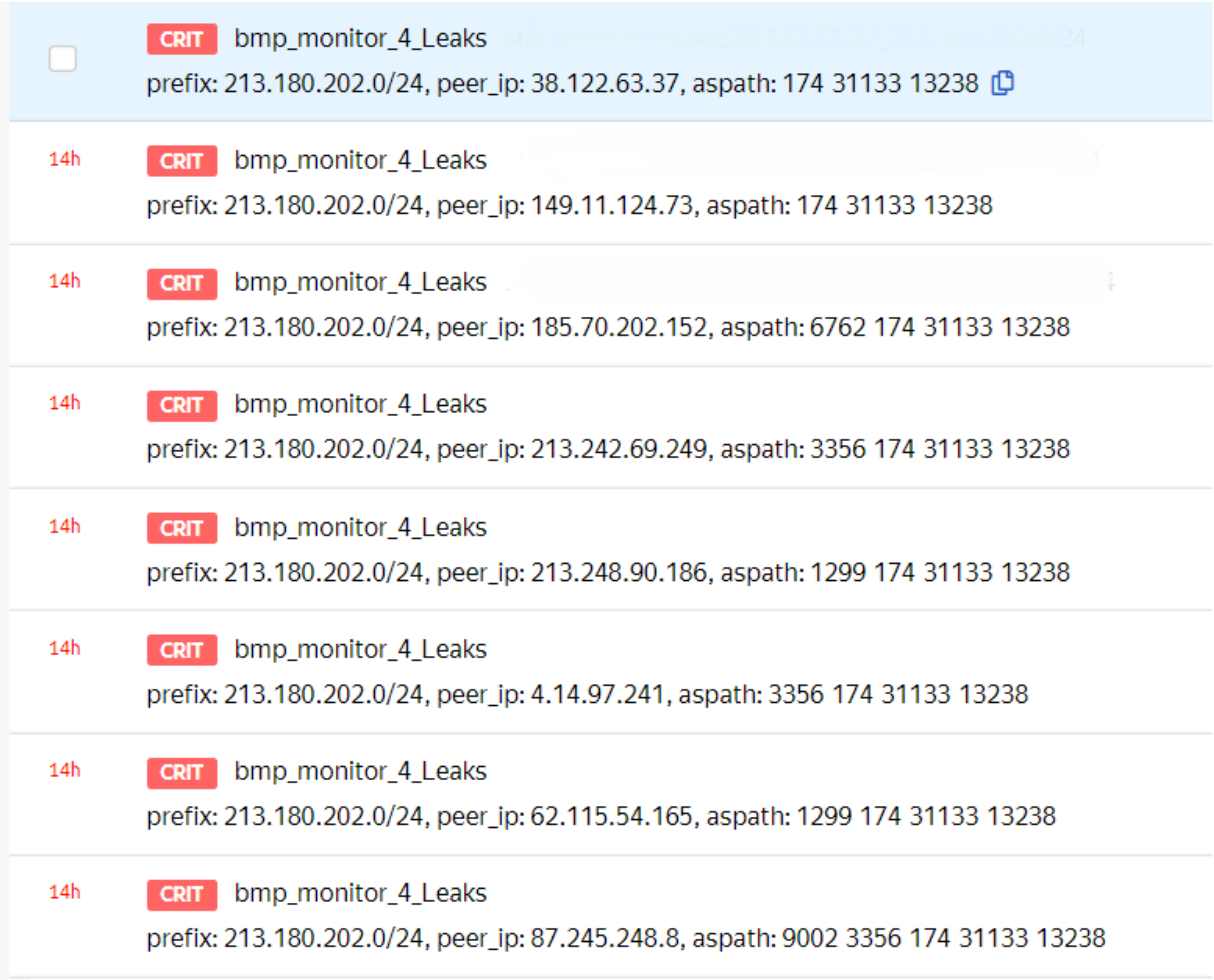
How Many ASPAs Do You Need?

15



Collector
Collector
Storage
SDK
ROA
rtrlib
Y-Detector
yaml
ASPA

Y-Detector: Proof of Concept



```
□     CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 38.122.63.37, aspath: 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 149.11.124.73, aspath: 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 185.70.202.152, aspath: 6762 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 213.242.69.249, aspath: 3356 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 213.248.90.186, aspath: 1299 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 4.14.97.241, aspath: 3356 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 62.115.54.165, aspath: 1299 174 31133 13238

14h   CRIT  bmp_monitor_4_Leaks
            prefix: 213.180.202.0/24, peer_ip: 87.245.248.8, aspath: 9002 3356 174 31133 13238
```

Infrastructure

We know when you leak!

Alexander Azimov, a.e.azimov@gmail.com