BGP Telemetry

CSNOG 2020

Telemetry?

Telemetry is …

A process of reading a quantitative data of some instrument and sending out those readings to some other entity.

- Telemetry is not a new concept in the (telecommunications) industry.
- Streaming telemetry and a trend of moving away from polling.

BGP?

BGP is …

[Hey, Ignas, remember where you are presenting this :-)]

BGP Telemetry

BGP works just fine (most of the time).

Visibility into BGP operation and especially BGP policy processing is limited.

MRT, SNMP traps, model based state, CLI, proprietary logging mechanisms.

Using BGP for monitoring BGP – dedicated BGP collector nodes, monitoring on reflectors, “looking glass” type of solutions.

Various streaming telemetry mechanisms for data plane and manageability are either well rooted or getting traction in the industry.

Can we do something similar with BGP too?

BMP - BGP Monitoring Protocol

- A dedicated protocol, not an extension of BGP
- Unidirectional, from network element to collector.
- Push model, information is streamed proactively without polling.
- Binary encoding, focus on lower load of a network element at a cost of higher load on a collector.
- Timestamped for event correlation.

The end result is visibility into BGP operation and convergence.

BMP Operation Model

Send out events and information related to BGP operation to an external entity.

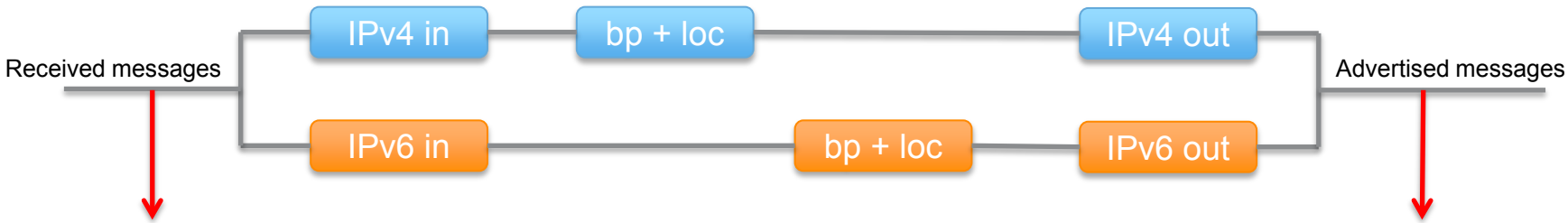
- Mirroring
- Events
- Monitoring
- Statistics

Feed everything to a collector, do not process it locally on the network element.

BMP feed provides enough of information for a collector to process received data at a later time.

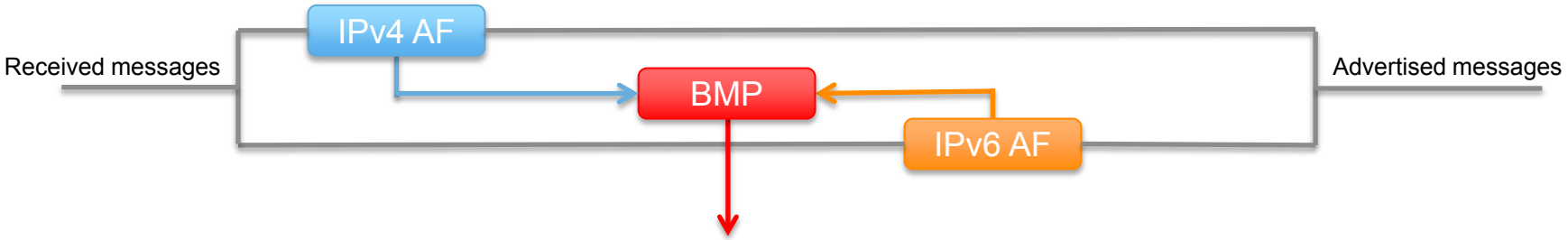
BMP: Mirroring

- An unmodified copy of BGP messages received or to be sent.
- BMP mirroring happens before BGP processing – a malformed message will be mirrored as is.
- Handy for tracking attribute and NLRI encoding errors and malicious attacks.
- BGP component will react to a malformed message as if there were no BMP present.



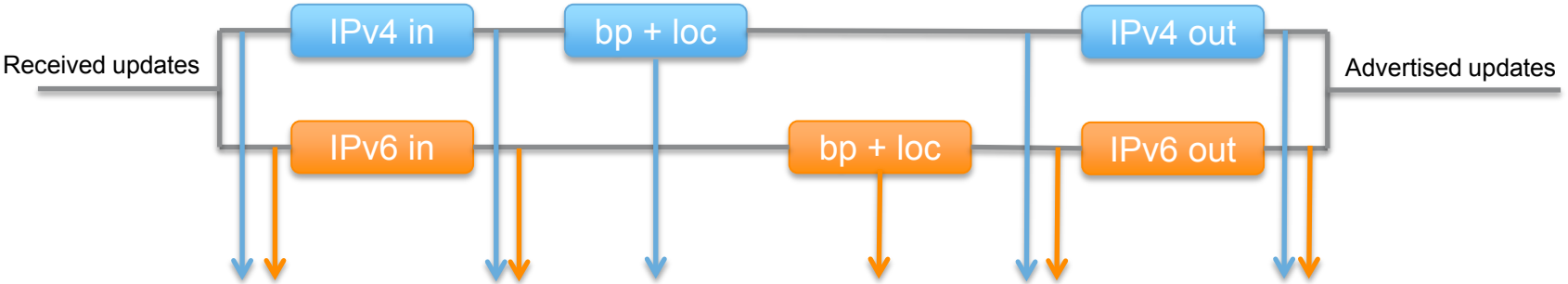
BMP: Events

- Peer up and down events, including actual exchanges of OPEN and NOTIFICATION messages.
- Collector receives authoritative information on session parameters.
- Events related to BMP operation: BMP generator overload conditions, administrative events.



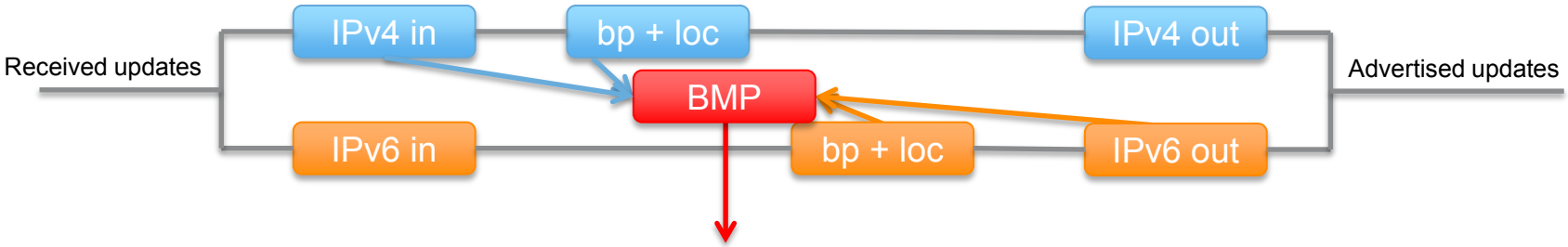
BMP: Monitoring

- Visibility into per-AF NLRI processing.
- Prefixes received pre- and post-policy, locally originated prefixes, and prefixes to be advertised pre- and post-policy.
- Including all the attributes – this allows for attribute tracking!
- Encoded as a regular BGP message – your existing toolchain may not require a major rework.



BMP: Statistics

- Per-AF counters of received, contained, and advertised prefixes – pre- and post-policy.
- Counters related to exception events – malformed, semantically incorrect or redundant announcements, loops in AS paths.
- Sent out periodically or on occurrence of some specific event condition.



BMP Deployment Aspects

- Software ecosystem: both generators and collectors need to be available for BMP to be of practical value.
- Most of credible network element vendors support BMP generator functionality.
- Strong collector ecosystem, both open and closed source.
- Industry is starting to accept BMP as a standard way of monitoring BGP.
- There may be redundant information – collectors need to be prepared to deal with it.
- Enabling BMP may impact network element and BGP operation – this is implementation specific.

Questions

- Why not JSON/XML/Protobuf/Thrift/my favourite encoding?
- What if my BMP session is lost?
- Is BMP lossless?
- Can we run a BGP session to a collector instead?
- Is this deployed at all?
- My BGP works fine, why bother?
- Why BMP is not (YANG) data model based?
- Can I use BMP for prevention of hijacks and leaks?
- This appears to generate lots of data?
- Privacy aspects?

Discussion

- Any other remaining questions?
- If you have already deployed BMP, what is missing?
- If you plan to deploy BMP, what is missing?