BGP monitoring

SIG-PMV Dublin 2019

Thomas Schmid
schmid@dfn.de
problem statement

- no history of BGP routing information
  - what? when? who?
- regular BGP session only announces best routes
  - CLI, netconf?
- ris.ripe.net and BGPplay only good for an outside perspective
- iBGPplay dead
- other tools commercial or complex or too simple
  - BGPmon
  - BGPreader
  - BGPstream
BGP monitoring protocol

- "Telemetry for BGP" over TCP
- RFC 7854, IETF GROW WG
- streams BGP information per BGP session, not per router as a normal BGP session would
- supports multiple AFs, e.g. BGP Linkstate
- gives ADJ-RIB-In pre-policy and post-policy
- unidirectional TCP session: nothing is sent to the router
- no best-path selection, i.e. no RIB
  - drafts for ADJ-RIB-Out and Loc-RIB
- more TLVs in the future

Cisco Config

```
bmp server 1
host 2.3.4.5 port 5000
update-source Loopback0
initial-delay 60
stats-reporting-period 300
initial-refresh delay 60 spread 120
!router bgp 680
  neighbor 1.2.3.4
    bmp-activate server 1
```
snas.io

- originally a Cisco-development, open-source
  - formerly known as openBMP using pnda.io
- https://github.com/SNAS/
  - chain of docker containers
  - python API for kafka
  - logstash integration etc.
out-of-the-box GUI features

- 12 dashboards
  - routing history
    - per AS, per Peer, per Prefix, per Router
  - top-lists
  - IRR/RPKI dashboards
    - violations, per-AS view
  - inventory
  - looking-glass
  - live AS-view
  - ...

SIG-PMV Dublin 2019
psql database

- + timescale DB
- accessible with standard management tools e.g. pgAdmin
- well structured and useful to build your own dashboards
  - customer views, iBGP, etc.
pros and cons

+ scales well
  - currently monitoring almost 2000 BGP sessions
    - Dell PowerEdge M640, 2 x Intel Xeon Silver 4110, 64GB, 500GB SSD
  - lightweight on the routers
    - no visible additional load when turning on BMP

+ easy to adapt to your specific needs
  - database has all the information you want

- no easy „full routing table view per router“
  - focus on changes per neighbor
  - BGP-table, not RIB
  - better use quagga and dump BGP table with caida tools BGPstream BGPreader for this purpose
  - stream mrt data to openbmp collector: mrt2bmp

- development stopped?
  - no updates since 6months, gitter chat quiet
    - but already a mature and good product
new monitoring DMON

▶ early stage. The dream:
  ▶ full integrated monitoring and substitution of existing monitoring tools: cacti, mrtg, log, ...
  ▶ full view over all network layers
  ▶ full root cause analysis of failures
  ▶ full alarming features
  ▶ great GUI

▶ source of truth: GIS
  ▶ central database, OSS/BSS for DFN
  ▶ all dependencies and processes already modeled
challenges

- GIS architecture outdated
  - 20 years
  - Adabas DB
  - single threaded
  - middleware CORBA
  - missing real-time APIs
    - mainly XML exports
- Telemetry later