Managing OOB networks

NLNOG Live!, 22 July 2020

This presentation slot

- Niels Raijer (Fusix Networks) will present the Fusix OOB network
- Job Snijders (NTT Communications) will present the NTT OOB network
- Both will discuss the merits and pitfalls of each other's OOB networks, and invite the audience to come up with questions and participate via chat
- As a result, we help the Internet become better managable!

Fusix Networks

- Operates two independent star networks in ~30 data centers in The Netherlands (decommissioned our USA network this year)
- Highly automated operation, small staff, lovely clients
- Reliance on meta-data for many tools in our automation platform Fusix Teamworks:
 - Customer portal with all kinds of info
 - Network automation platform for provisioning, deprovisioning and operation

An OOB network?

- That's just to connect to your equipment in case there is a problem, right?
- Right.

Until it isn't.

- SNMP polls/traps
- sFlow/Netflow (DDOS detection)
- BGP session monitoring
- Configuration updates
- VPN access (if a tool doesn't need to be reached from outside, why run it on a public IP)?
- Internal DNS view
- Emergency CLI access via SSH / console

The usual methods don't cut it

- Getting small-commitment ethernet ports from the neighbors in the rack next door (cross connect cost)
- Putting a 4G router in each rack (coverage, scalability, stability)
- DSL lines (have you ever tried to get a DSL line in a data center?)

So we built an in-band out-of-band

- Locations where we have dark fiber: we use one WDM wave specifically for OOB
- Locations where we lease a wave: we configure one VLAN specifically for OOB

Redundancy via BGP

- Two Juniper SRX core OOB routers (each in its own private AS)
- Each data center has an OOB router; each OOB router has its own private AS and announces a /24 of private IP space to both cores over the OOB WDM wave or OOB VLAN
- The management ports of our switches, ethernet ports of our Air Console servers, and the management ports of the power bars (where applicable) all connect to the OOB router in the /24
- Since we always have at least TWO dark fibers or TWO leased waves to each location, the setup is redundant
- Bonus: since we monitor the status of the OOB BGP sessions, we have a crude fiber cut detection system

Access to the OOB

- Via servers connected to public IP and to the OOB (one in our own network, and a further two connected to friendly competitor's networks), running OpenVPN
- Direct connectivity from our office (where we have leased fiber to NIKHEF) – basically our office acts as if it was a data center location, too

Services in the OOB

- Internal DNS view
- Monitoring via LibreNMS and friends
- All software tools for configuration changes, flow tools, customer portal, etc. running on VM clusters in the OOB

Are you happy running your IB OOB?

- Yes.
- Well. After replacing the original Mikrotik core OOB routers with SRX that is.
- The Mikrotik just kept thinking it was a layer 2 device whatever the config. You don't know what a bad day is until you had a loop on your OOB.
- Since replacing the Mikrotik our OOB uptime is 100%.

Any lessons for us? What would you improve?

- Running an in-band out-of-band network is feasible.
- Don't use a layer-2-loving device as a core router though.
- Improvements: implement RPKI on our OOB of course! ③
- I think we are pretty close to perfection. I'd love to hear your thoughts.