BYOI (Bring your own incident) - Deutsche Telekom

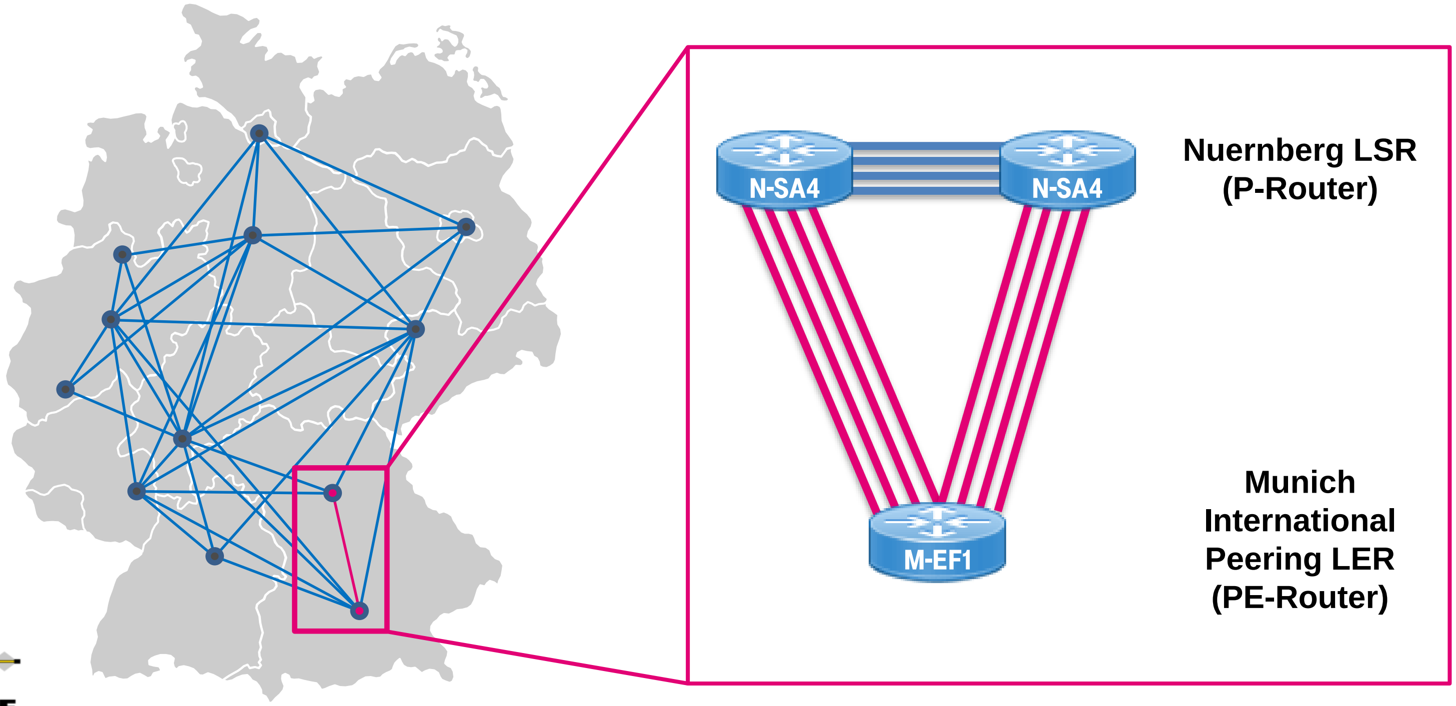
TOP-URGENT 24-12-007:
MPLS blackholing due to Software bug

IETF122 – Bangkok

Holger Keller, Nils Warnke

I E T F

WHERE did this happen – IP Backbone Germany



I E T F

Situation leading to Issue

- All parallel IP-Trunks to the upstream LSRs have been deactivated for maintenance reasons by setting the ISIS metric to 10 million
- After maintenance was completed, the uplinks were re-configured with the correct ISIS metric for forwarding
- The configuration was executed via Orchestrator with automated workflows, triggering all connections separately (means separated commits on the router)

22: Activate "4P2//49/89/786...	4P2//49/89/7861/7Y41//...	ip-trunk-cfs_7.0.17301...	Inactive	Active	Completed		100%	2024-12-16 08:
22: Activate "4P2//49/89/786...	4P2//49/89/7861/7Y41//...	ip-trunk-cfs_7.0.17301...	Inactive	Active	Completed		100%	2024-12-16 08:
22: Activate "4P2//49/89/786...	4P2//49/89/7861/7Y41//...	ip-trunk-cfs_7.0.17301...	Inactive	Active	Completed		100%	2024-12-16 08:
22: Activate "4P2//49/89/786...	4P2//49/89/7861/7Y41//...	ip-trunk-cfs_7.0.17301...	Inactive	Active	Completed		100%	2024-12-16 08:
22: Activate "4P2//49/89/786...	4P2//49/89/7861/7Y41//...	ip-trunk-cfs_7.0.17301...	Inactive	Active	Completed		100%	2024-12-16 08:

Detecting the issue

- From change management perspective all pre- and post checks were successfully completed
- Internal alarms were not triggered in DT’s monitoring systems
- 20 minutes after bringing connections back into routing, direct customer complaints were received and we additionally saw an anomaly from external data source.

I E T F

Root cause analysis

- Challenge: Identify that the issue was triggered by a change
  - In the meantime, incident team decided to roll-back all backbone related changes
- Human anomaly detection: 3rd level Operator suspected that incident could be related to MPLS blackholing (out of experience).
- Re-applying the ISIS metric triggered a router OS software bug causing traffic blackholing.
  - The ingress line card uses a different next-hop ID than the egress line card.
  - When the traffic reached the egress line card / egress NP, it cannot process the packet and drops the traffic.

I E T F

What did we learn from the issue?

- (SR-) MPLS forwarding Monitoring across multiple ECMP paths is a complex task and currently not solved for DT.
  - Blackholing is a rare case yet with high customer impact
- STAMP or TWAMP based flow monitoring could potentially be an option and are being analyzed.
- Advancing standardized vendor agnostic solution on operator side required.
  - Need for end-to-end service and network observability in near real-time even more relevant than a few years ago.

I E T F