



# Swisscom Network Analytics

## Why Network Modelling with Digital Map is the next step

23.07.2023, Thomas Graf – [thomas.graf@swisscom.com](mailto:thomas.graf@swisscom.com)

*Picture: Apollo 8, December 24th 1968*



# Nationwide Network Outages everywhere

Increasing in impact and duration - hinting Network Visibility deficiencies

## Canada: Rogers says network upgrades after outage will cost \$261M, but no timeline given

By Staff - The Canadian Press  
Posted August 25, 2022 11:09 am



Rogers CEO Tony Staffieri explained to a standing committee in the House of Commons on Monday that the technology...  
C-7: Rogers Communications Service Outages  
Pannes de service de Rogers Communications  
Global NEWS  
00:05 / 02:23  
Rogers CEO Tony Staffieri explained to a standing committee in the House of Commons on Monday that the technology...  
C-7: Rogers Communications Service Outages  
Pannes de service de Rogers Communications  
Global NEWS  
00:05 / 02:23

## Swisscom boss apologises for massive network outage - newspaper

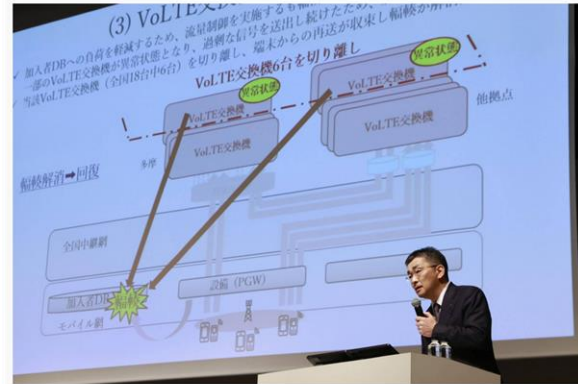
Reuters

2 minute read



1/2  
Chief Executive Urs Schaeppi of Swisscom, mobile phone and digital television provider Swisscom addresses the company's annual news conference in Zurich, Switzerland February 7, 2019. REUTERS/Arnd Wiegmann

## Japan: KDDI to spend ¥7.3 billion to compensate users for major network outage



KDDI chief Makoto Takahashi speaks to reporters in Tokyo on Friday. | KYODO

BY KAZUAKI NAGATA

SHARE Jul 29, 2022

05 FEB 2023 | 08:23 AM UTC

## Italy: TIM internet services interruption reported nationwide Feb. 5

TIM internet services interruption reported in Italy Feb. 5. Likely communication disruptions.

Informational Communications/technology Transportation ITA

## France: ORANGE FRANCE UNDER FIRE FOR MISHANDLING NETWORK OUTAGE

Posted by Harry Baldock | Jul 22, 2021 | Subsea, INFRASTRUCTURE, Satellite, Towers, COMPANY NEWS, Governance, Data Centres, Networks, Wholesale, Virtualisation, Europe, Middle East & Africa, News



## Facebook outage: what went wrong and why did it take so long to fix after social platform went down?

Billions of users were unable to access Facebook, Instagram and WhatsApp for hours while the social media giant scrambled to restore services



Facebook, Instagram and WhatsApp all went down, and reappeared online after a six-hour global outage. Photograph: Anadolu Agency/Getty Images





**The customer knows before Swisscom that there is service interruption.**

**Unable to recognize impact and root cause when configurational or operational network changes occur.**

**Swisscom suffers reputation damage.**  
**We need to work together to mediate.**



**Markus Reber**

Head of Networks at Swisscom



*“ It is our duty to recognize service interruption  
before our customer does.*

*Why do we still often fail to be first ? “*





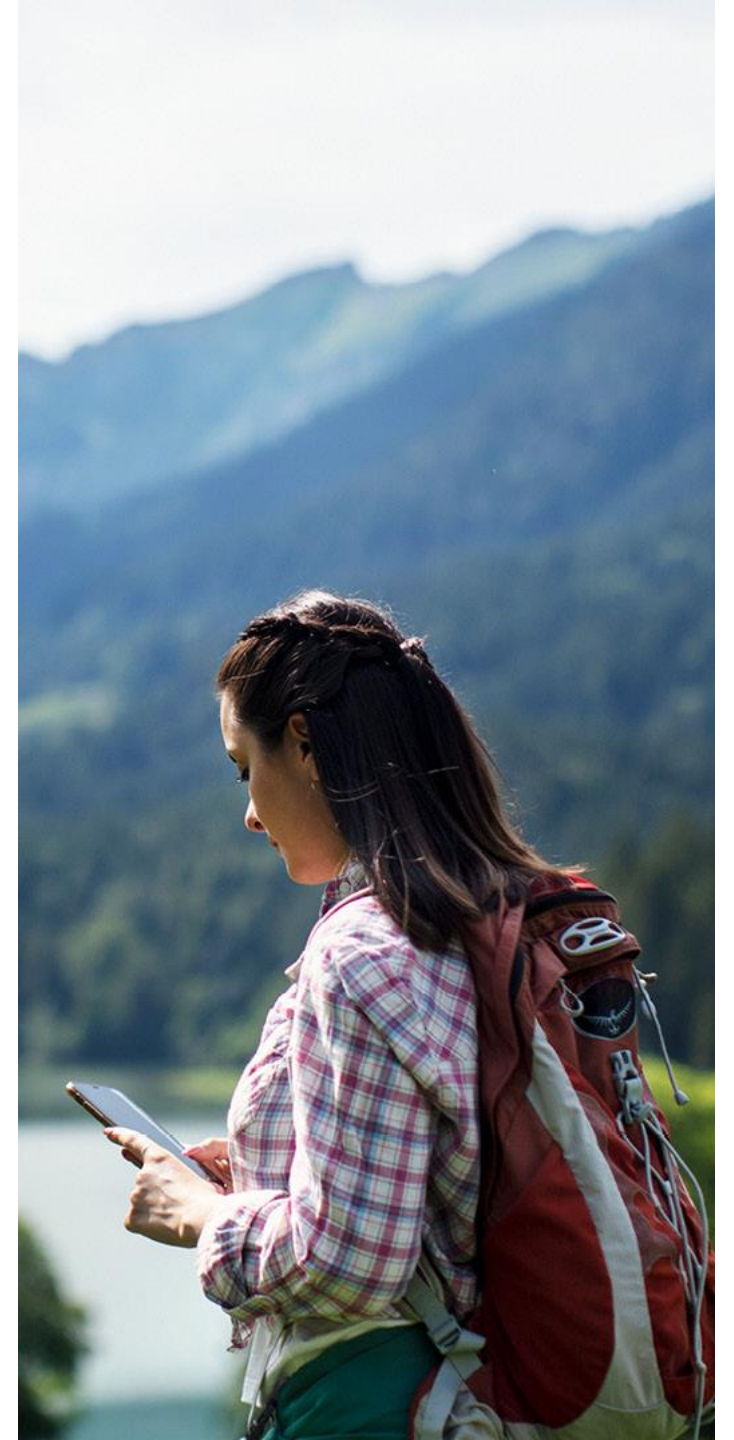
From Network Analytics Postmortems we understood that roughly 50% of the major network incidents are configuration related.

Network engineers **unable to understand all the end-to-end dependencies on all the layers** in highly virtualized networks.



**Thomas Graf**

Distinguished Network Engineer  
and Network Analytics Architect at Swisscom







Within an 8 months Network Anomaly Detection Proof of Concept, we observed that reaction times to operational and configurational changes in the network was reduced, but also **initial context helped to quicker identify the root cause.**


**To further improve, ietf-network.yang and ietf-network-topology.yang defined in RFC 8345 details network modelling, especially on configurational aspects.**

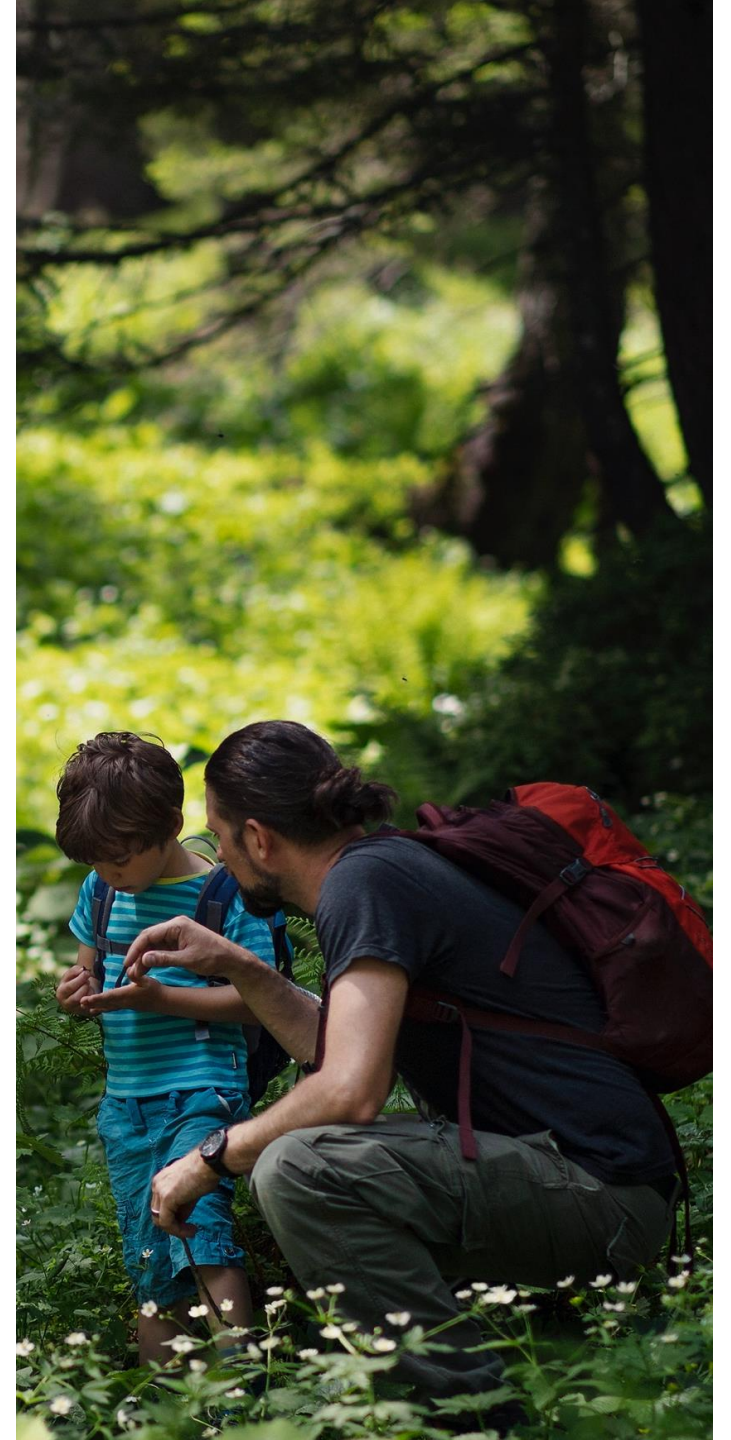


**Thomas Graf**

Distinguished Network Engineer  
and Network Analytics Architect at Swisscom



The Digital Map, draft-havel-opsawg-digital-map, points correctly out **that missing Bidirectional links and support for Multi-point connectivity in RFC 8345 ietf-network-topology.yang** makes the implementation rather complicated or even renders certain topologies as unusable. 







« And finally, and most importantly, with the Digital Map network modelling, **the foundation for simulating network configuration changes in lab** is at reach. Preventing networking incidents from evening happening.

**Resolving the problem that lab environments are never identical to production network.**







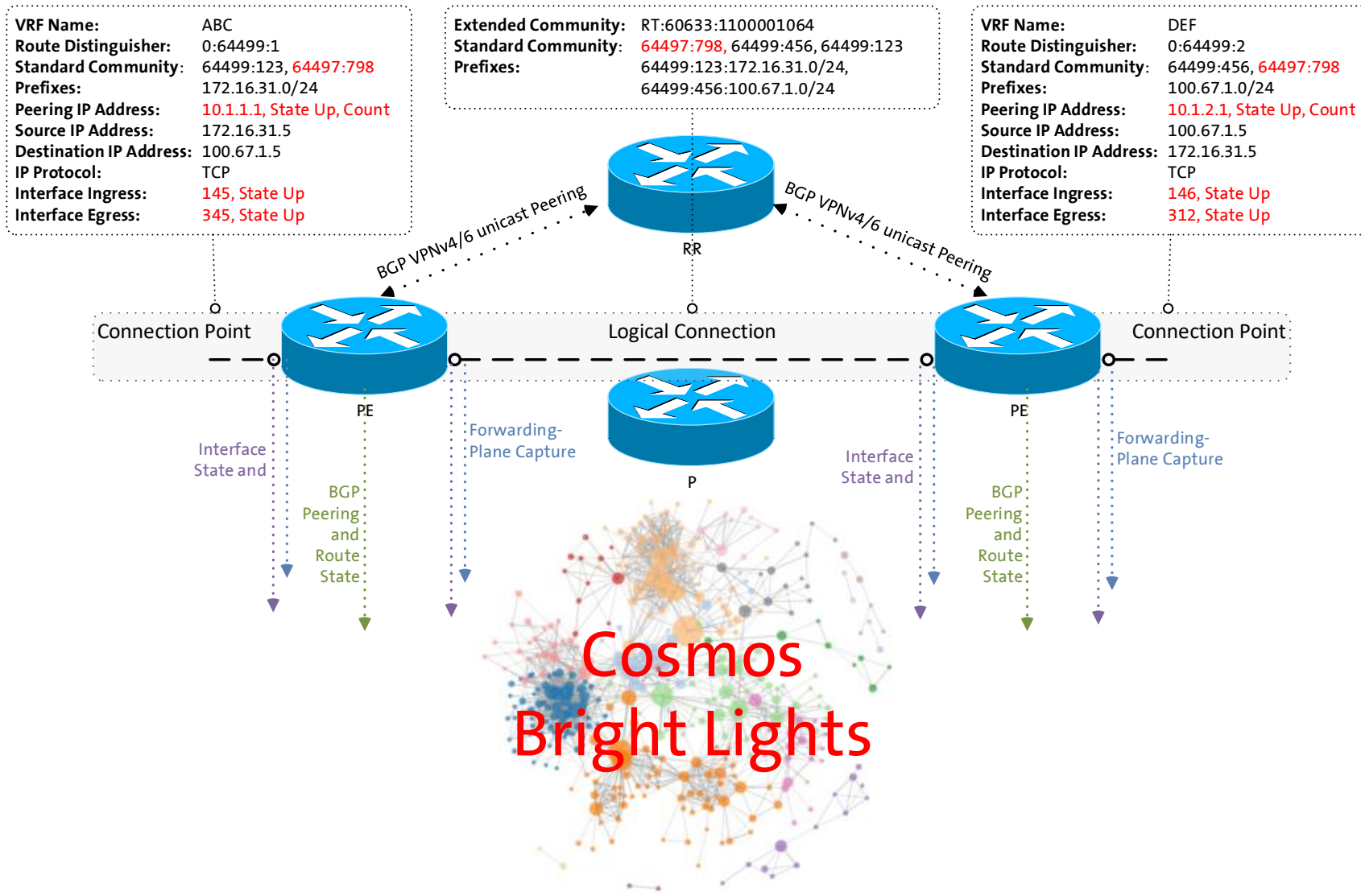
*“ Without network visibility,  
no informed decisions can be made. “*





# Monitor L3 VPN Relationships in Near Real-Time

What Interfaces are for Flows, Peerings are for BGP



- **Interface State** - Determine which Interfaces belong to the L3 VPN and track their state.
- **BGP Peering State** - Determine which BGP peerings belong to the L3 VPN and track their state.
- **BGP Updates/Withdrawals** - Determine which BGP paths belong to the L3 VPN and track their state.
- **Traffic Drop** - Determine which traffic flows belong to the L3 VPN and track wherever the dropped byte count spikes.
- **Flow Count Change** - Determine which traffic flows belong to the L3 VPN and track wherever the flow count drops or spikes.
- **Missing Traffic** - Determine which traffic flows belong to the L3 VPN and compare the forwarded byte count to previous week.



1. **A single link down** result in multiple device topology, control-plane and forwarding-plane events being exposed at different times.

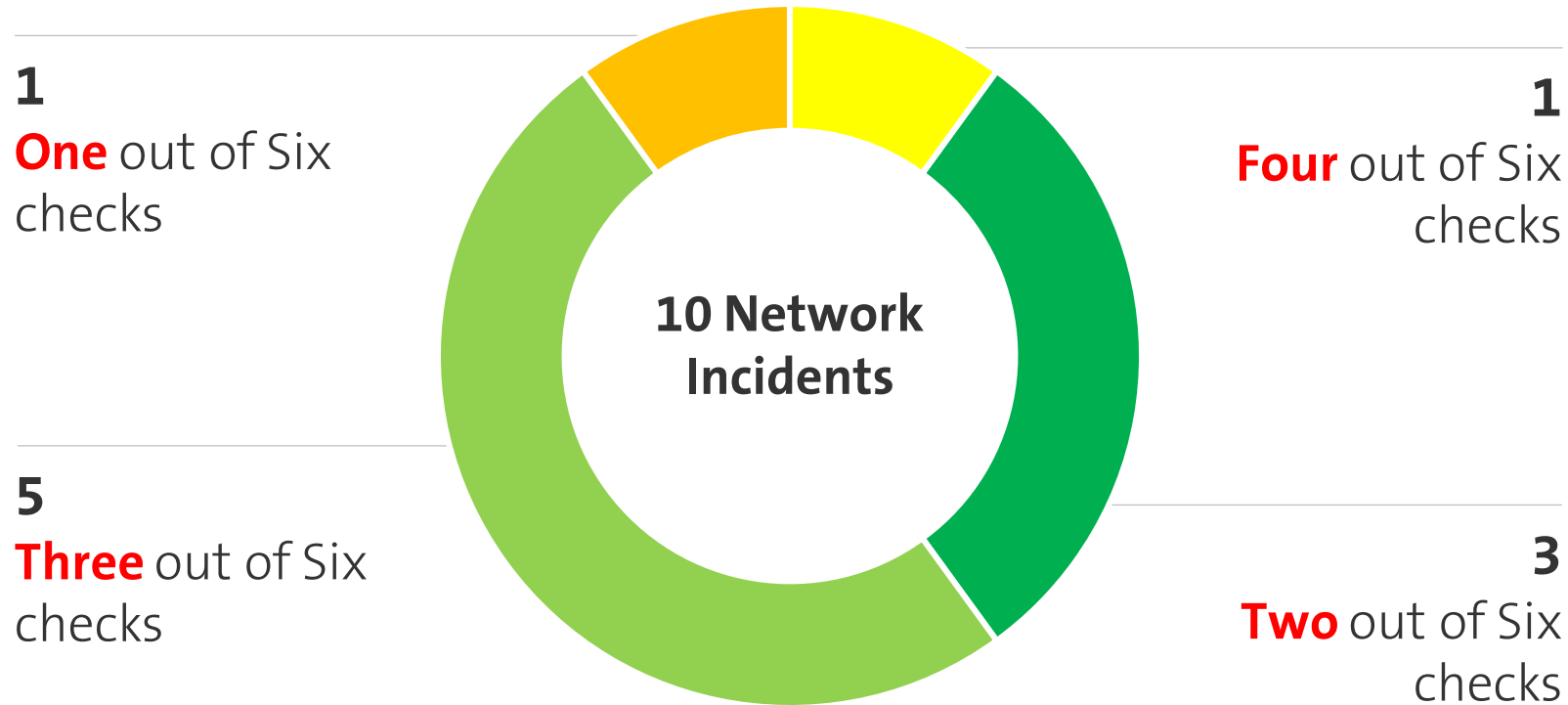
- 
- The diagram illustrates the Network Event Alert Unification Framework, which consists of four sequential stages:
- 1 Network Event**: This stage shows a network topology with six blue circular nodes (routers) connected by lines. Three specific events are highlighted:  $T_2$  (orange dashed arrow from the first node),  $T_1$  (blue dashed arrow from the second node), and  $T_3$  (purple dashed arrow from the third node).
  - 2 Observation Strategy**: This stage receives input from the Network Event stage. It features a magnifying glass icon, indicating a search or analysis phase. The inputs are represented by dashed arrows: orange for  $T_2$ , blue for  $T_1$ , and purple for  $T_3$ .
  - 3 Concern Scoring**: This stage receives input from the Observation Strategy stage. It features a head with a gear icon, indicating a cognitive or scoring process. The inputs are represented by dashed arrows: orange for  $T_2$ , blue for  $T_1$ , and purple for  $T_3$ .
  - 4 Alert Unification**: This stage receives input from the Concern Scoring stage. It features an envelope icon, indicating the final output or notification. The inputs are represented by dashed arrows: orange for  $T_2$ , blue for  $T_1$ , and purple for  $T_3$ .
- The final output of the framework is a large black arrow pointing downwards, indicating the final result or action.





# Network Anomaly Detection PoC Detail

Multiple Perspectives increases Accuracy



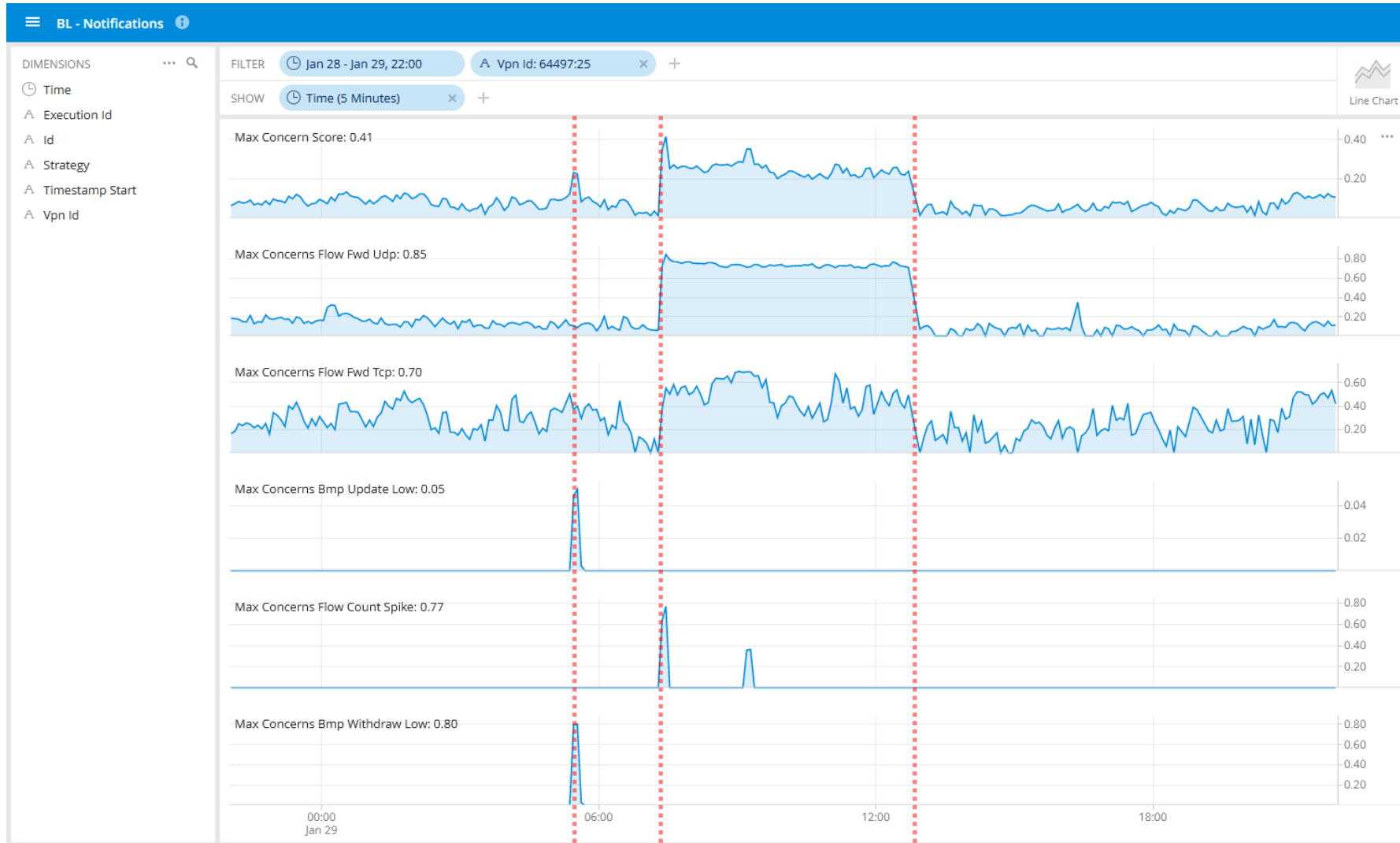
## Key Facts

- > **Networks are deterministic, Customers somewhat holds true.**
- > Max Concern score ranged between 0.25 and 0.85. In average 0.46.
- > Incident patterns are repetitive. Month by month scoring improvements visible.
- > Individual expert rule accuracy is beyond 90%. Summed accuracy is beyond 95%.
- > Record and Replay Digital Twin works like a charm.
- > In 4 cases additional YANG, in 2 cases additional BMP, in 2 cases Netconf Transaction-ID and 1 case additional L2 IPFIX metrics would have helped to gain more visibility.
- > **Presented at ANRW 2023 at IETF 117 on Monday July 24<sup>th</sup> 15:30 – 17:00.**



# January 29<sup>th</sup> 2023, B2B Customer LAN-I Secure CER Traffic Blackholing

## Logical Connection 785 - L3 VPN monitored By Network Anomaly Detection





**Imagine** that with such a Network Anomaly Detection alert, **a reference to the Digital Map is included, dependencies are being shown in real-time and you can play the changes backwards in time.**

