Swisscom Network Analytics
Why Network Modelling with Digital Map is the next step

23.07.2023, Thomas Graf – thomas.graf@swisscom.com
Picture: Apollo 8, December 24th 1968

swisscom

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 outage: CEO outlines investments company is making to avoid fu...
Rogers CEO Tony Staffieri explained to a standing committee in the House of Commons on Monday tha...

Rogers Communications Service Outages | Pannes de service de Rogers Communications

Rogers CEO Tony Staffieri explained to a standing committee in the House of Commons on Monday that the technology

Media & Telecom

Swisscom boss apologises for massive network outage - newspaper

Reuters

2 minute read

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

BUSINESS

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

(3) VoLTE交換機
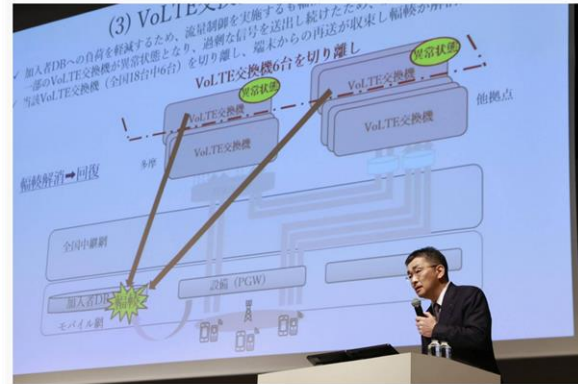
KDDI chief Makoto Takahashi speaks to reporters in Tokyo on Friday. | KYODO

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

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 ?"
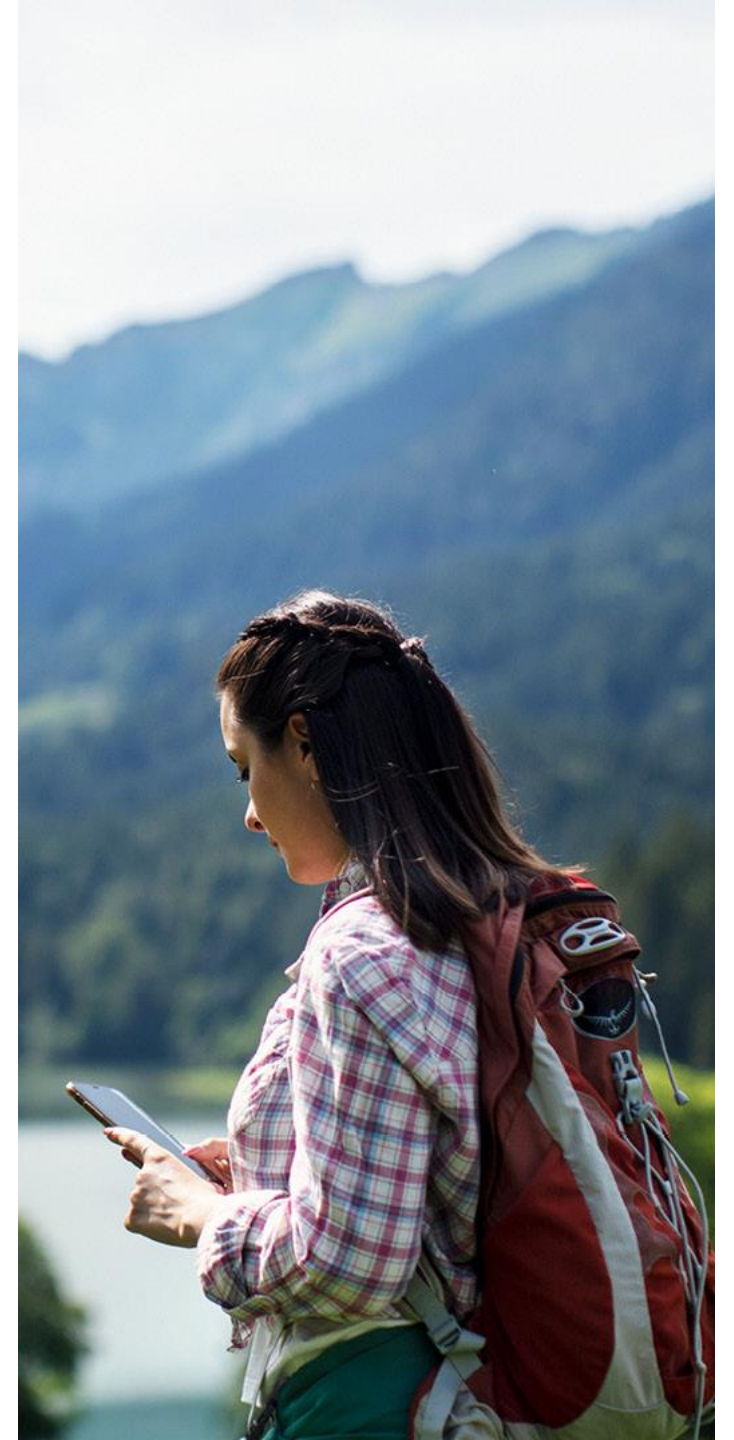
«

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 defined in RFC 8345 details network modelling, especially on configurational aspects.
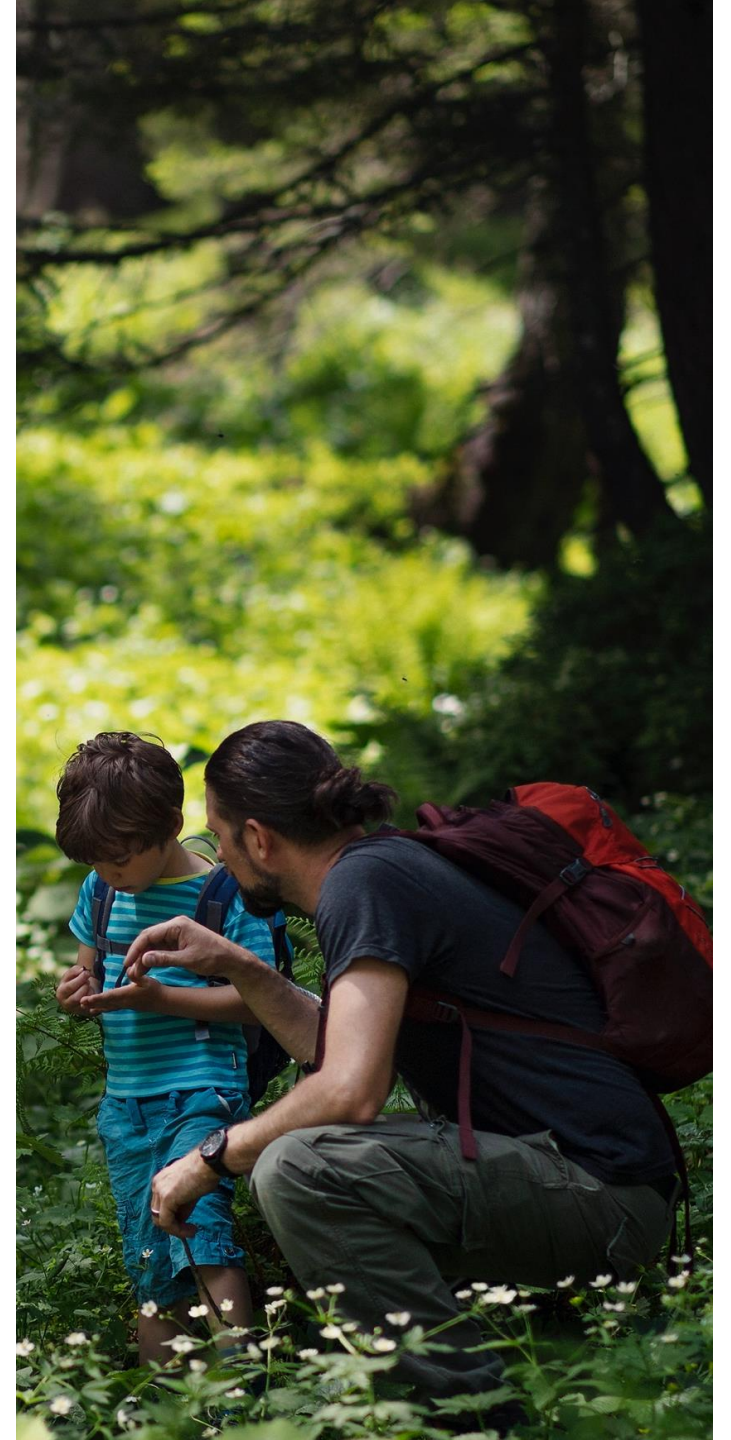
»

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.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. »
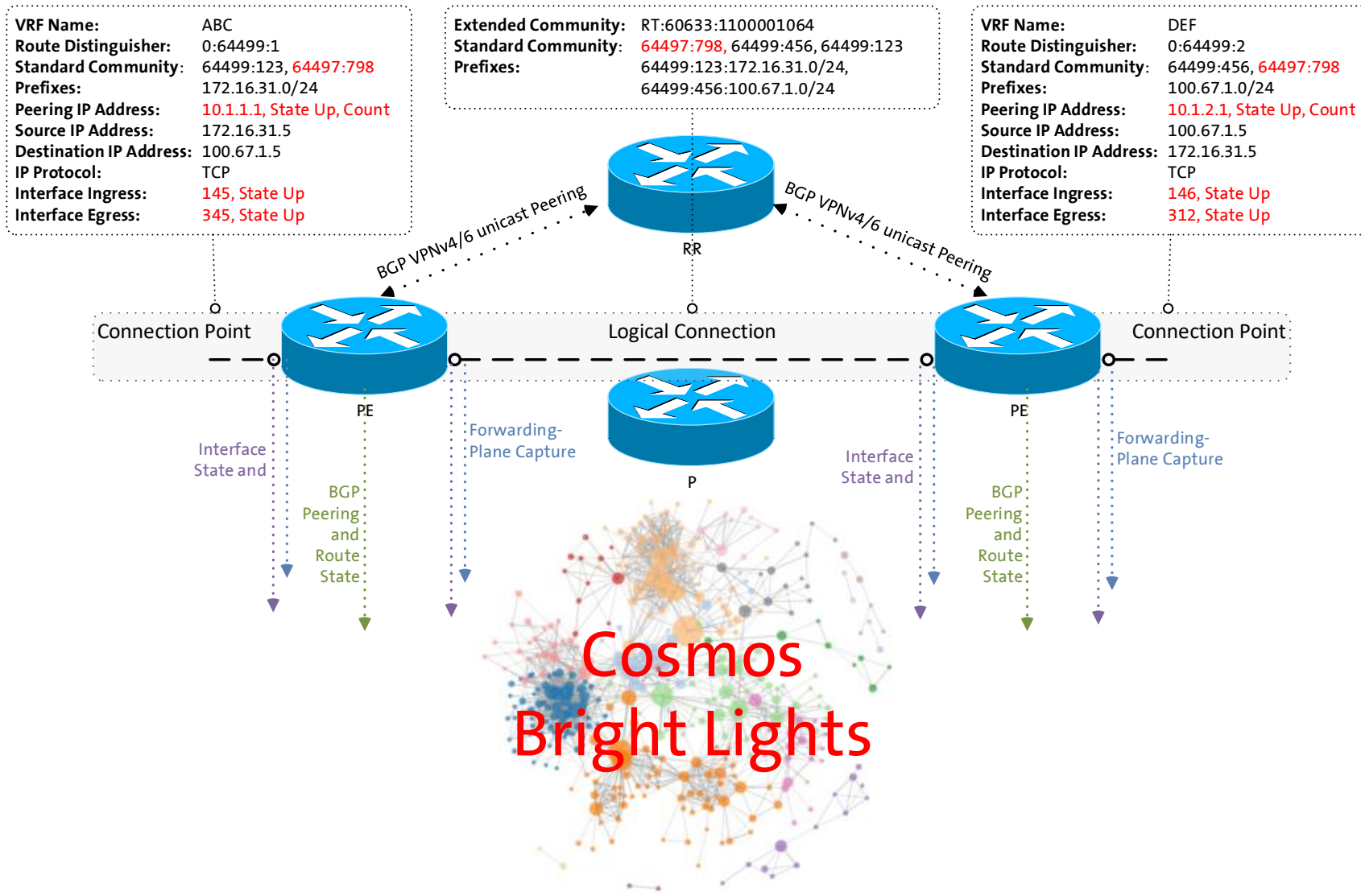
" Without network visibility,

no informed decisions can be made. "

Monitor L3 VPN Relationships in Near Real-Time
What Interfaces are for Flows, Peerings are for BGP

VRF Name:	ABC
Route Distinguisher:	0:64499:1
Standard Community:	64499:123, 64497:798
Prefixes:	172.16.31.0/24
Peering IP Address:	10.1.1.1, State Up, Count
Source IP Address:	172.16.31.5
Destination IP Address:	100.67.1.5
IP Protocol:	TCP
Interface Ingress:	145, State Up
Interface Egress:	345, State Up

Extended Community:	RT:60633:1100001064
Standard Community:	64497:798, 64499:456, 64499:123
Prefixes:	64499:123:172.16.31.0/24,
	64499:456:100.67.1.0/24

VRF Name:	DEF
Route Distinguisher:	0:64499:2
Standard Community:	64499:456, 64497:798
Prefixes:	100.67.1.0/24
Peering IP Address:	10.1.2.1, State Up, Count
Source IP Address:	100.67.1.5
Destination IP Address:	172.16.31.5
IP Protocol:	TCP
Interface Ingress:	146, State Up
Interface Egress:	312, State Up

BGP VPNv4/6 unicast Peering

BGP VPNv4/6 unicast Peering

RR

Connection Point

Logical Connection

Connection Point

PE

PE

P

Interface State and

Forwarding-Plane Capture

Interface State and

Forwarding-Plane Capture

BGP Peering and Route State
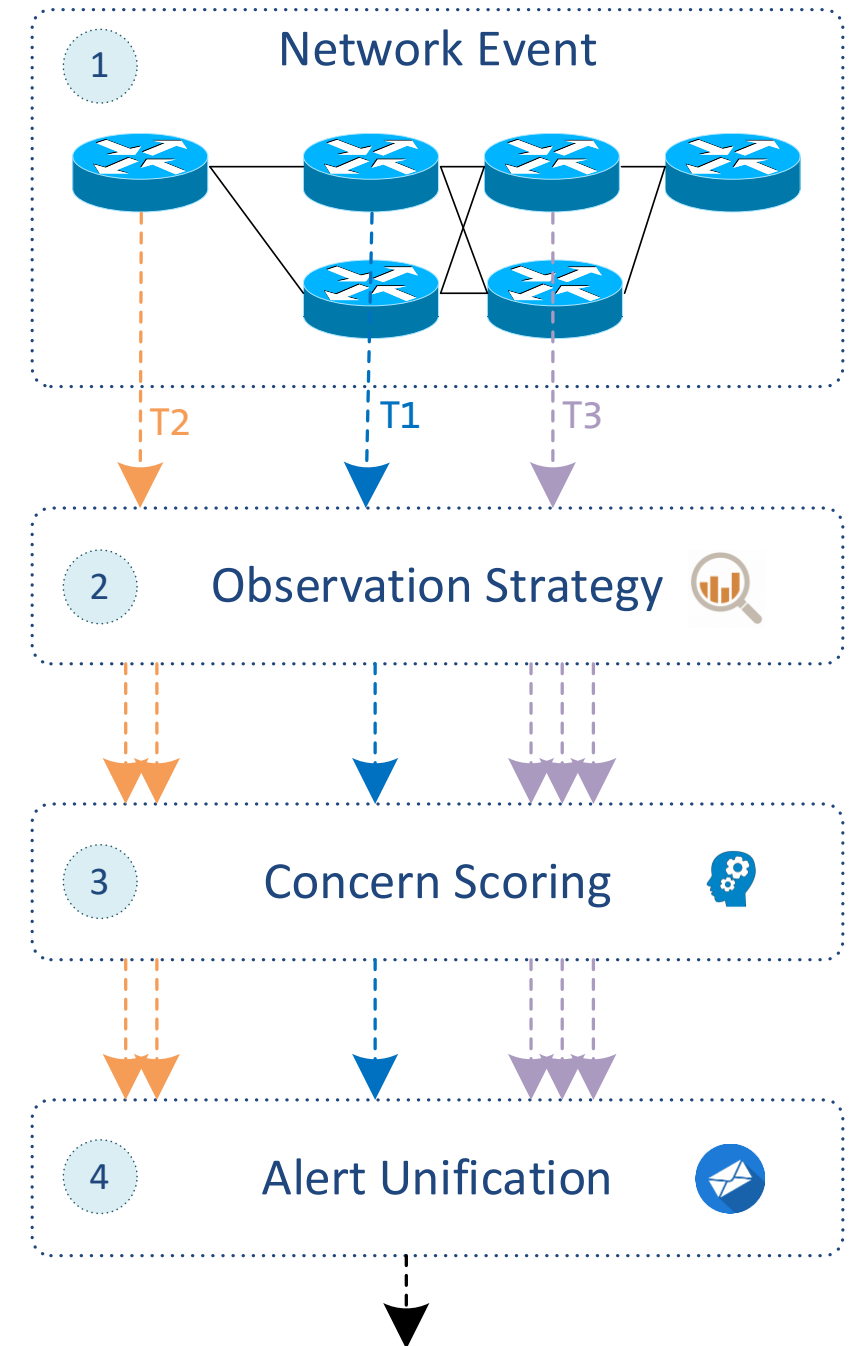
BGP Peering and Route State

Cosmos
Bright Lights

> **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.

From Network to Alert Event
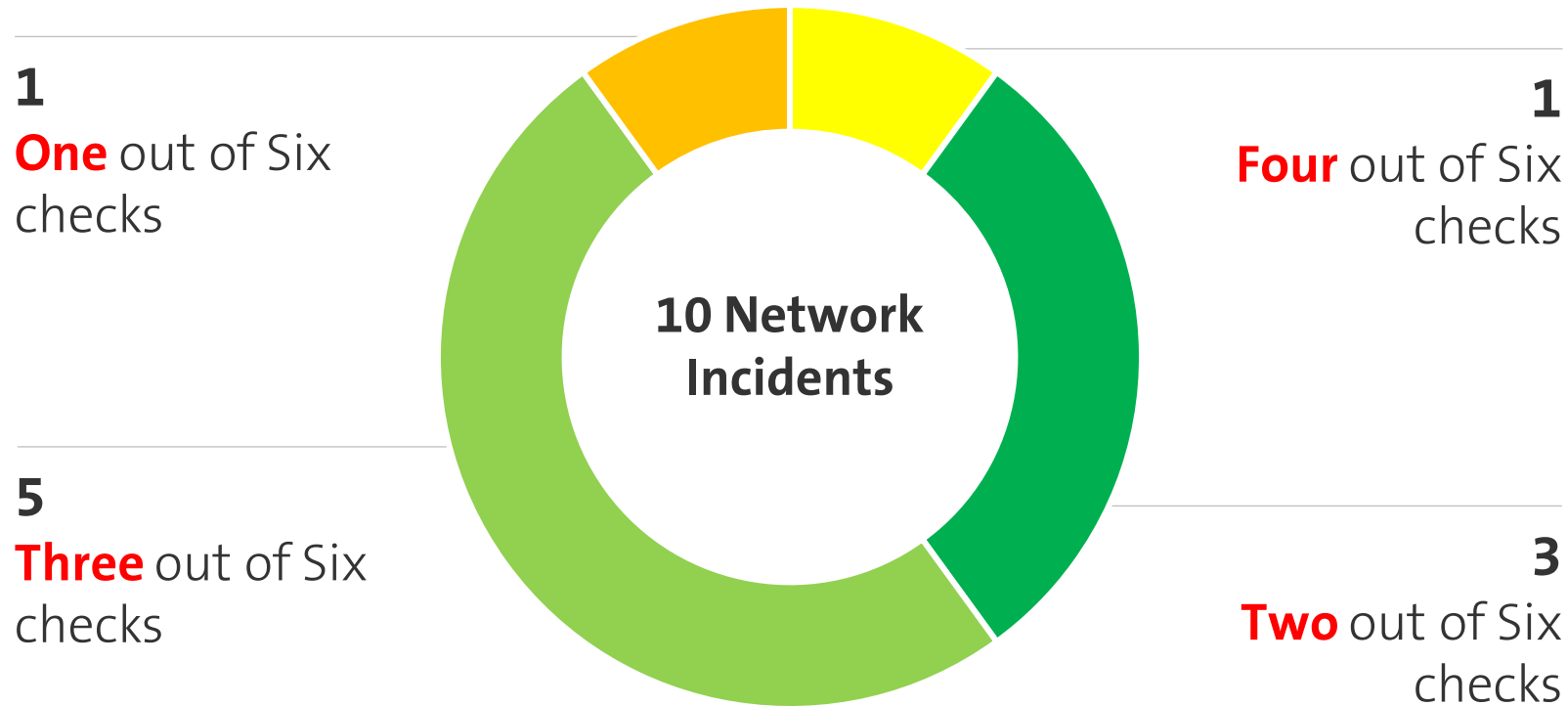Observe multiple perspectives at different times

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

2. **Determine** which interfaces and BGP peerings are being used first and then observe state. **Observe** BGP withdrawals and updates, traffic drop spikes and missing traffic. Generate multiple concerns.

3. **Calculate** for each check a concern score between 0 and 1. **The higher, the more probable** the changes impacted forwarding.

4. **Unify** several concerns for one VPN connectivity service to one alert identifier.

Network Anomaly Detection PoC Detail
Multiple Perspectives increases Accuracy

1
One out of Six checks

1
Four out of Six checks

10 Network Incidents

5
**Three** out of Six checks

3
Two out of Six checks

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 24th 15:30 – 17:00.**

January 29th 2023, B2B Customer LAN-I Secure CER Traffic Blackholing
Logical Connection 785 - L3 VPN monitored By Network Anomaly Detection

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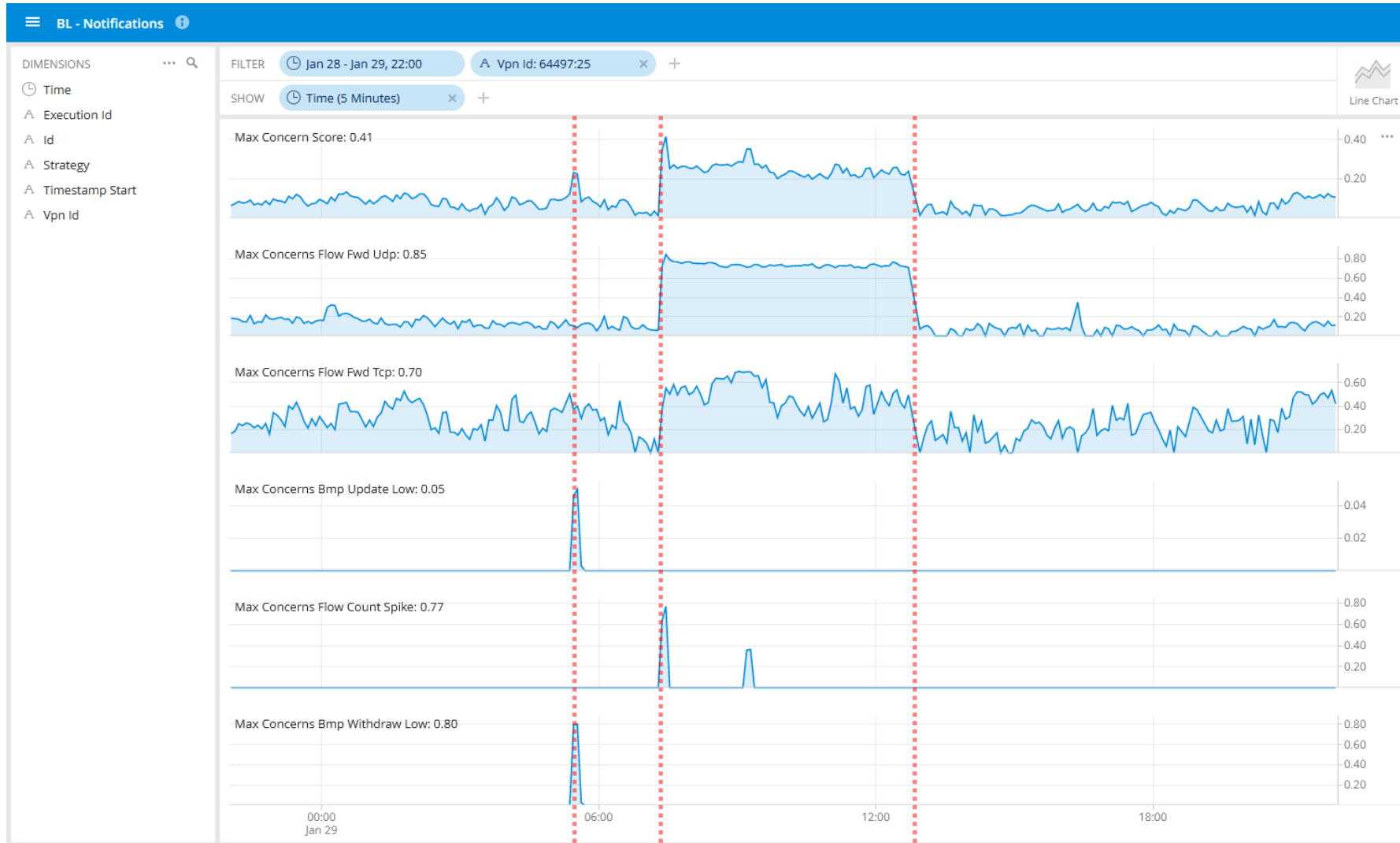
Imagine that with such a Network Anomaly Detection alert, **a reference to the Digital Map is included, dependencies are being shown in real-time and you can play the changes backwards in time.**

»