Network Observability

Why Should I Care, What Should I Care About?

an stateful perspective

dinesh g dutt, stardust systems

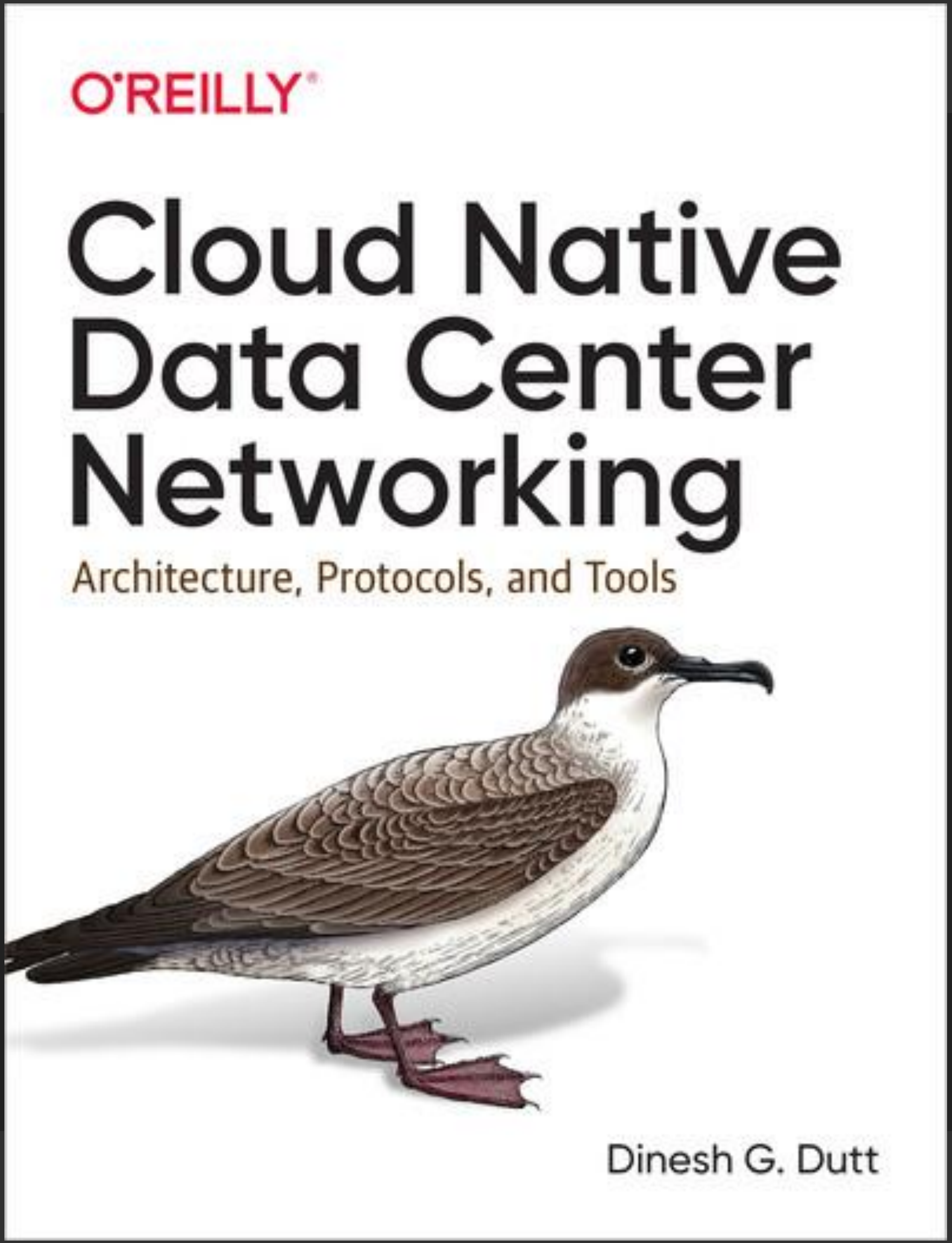
Feb 7, 2024

Cisco Systems

CUMULUS

SUZIEQ

A fundamental problem with networking today: getting a systemic view of the network, and acting on it network observability: the ability to answer any question about your network



O'REILLY

Cloud Native Data Center Networking

Architecture, Protocols, and Tools

Dinesh G. Dutt

How Does Network Observability Help?

Systemic (Fabric?) wide view of the network

Network Documentation

Network Validation

Troubleshooting Network Behavior

Audits and Compliance

Observability requires gathering far more data than traditional monitoring

State, metrics, packet flow, packets, logs

Its 2024, and yet pulling data from devices is like pulling teeth

Especially state data

the myth: vendors will all come together and develop a standard to provide a vendor-neutral way to export data from devices

zippiknits.blogspot.com

snmp

netconf/yang (SNMP with XML)

openconfig (my xml is better than yours)

gnmi (i can push my better encoding/rpc)

yang push (I can shove your push)

Other encodings (plus ca change,..)

Are we approaching pulling data from networks with the wrong models?

Network protocols need interop, data export does not

“I very frequently get the question:
'What's going to change in the next 10 years?'

And that is a very interesting question; it's a very common one. I almost never get the question:
'What's not going to change in the next 10 years?'

And I submit to you that that second question is actually the more important of the two -- because **you can build a business strategy around the things that are stable in time**…”

jeff bezos

what’s not going to change?

vendor differentiation

developers need to debug

devices have a long tail life

vendor-specific, and consistent data models and outputs make sense

What can vendors do?

Treat observability as a feature

Not change outputs for inconsequential reasons

Provide command options to return all data (show ip arp vrf all, for eg)

What can standards do?

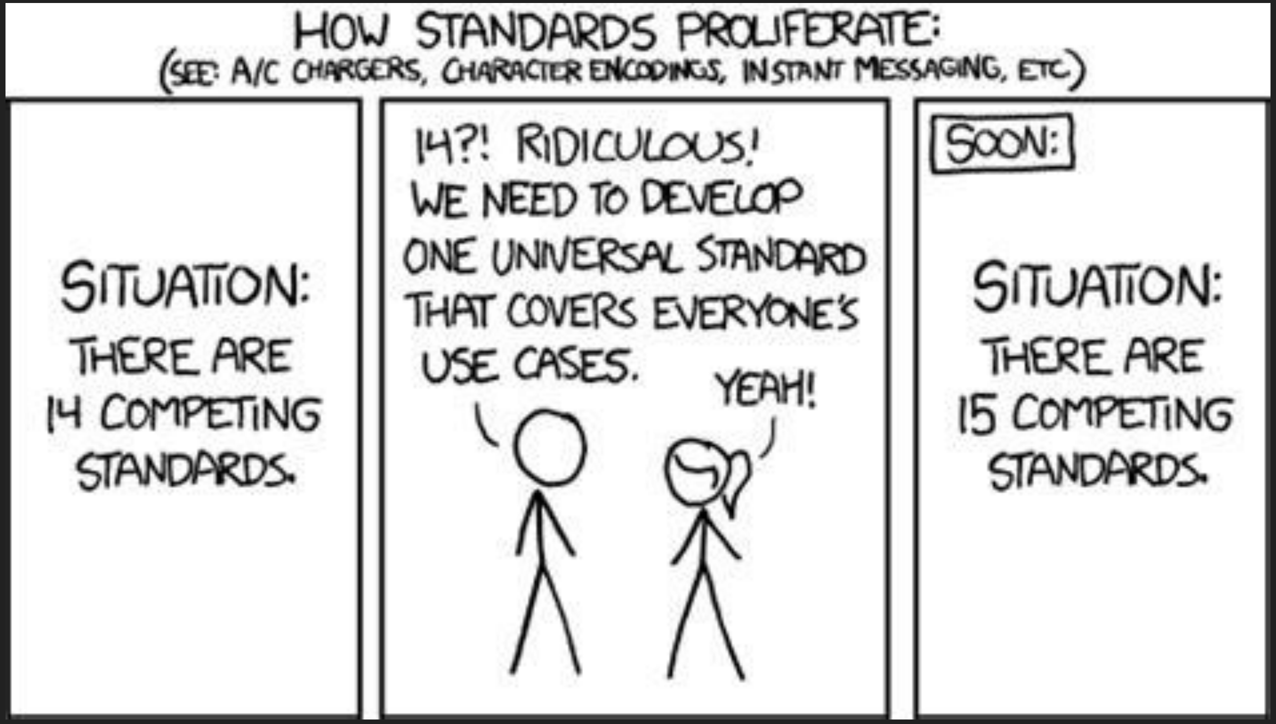
Have vendors submit their model and have them stick to it (think IANA rather than BGP WG)

What can operators do?

Treat observability as a required feature

Demand vendors not change outputs for inconsequential reasons

lets not do work that lands us on an xkcd cartoon


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

dinesh@stardustsystems.net

Network Observability Enterprise Perspective

Mike Ackermann,   INTC /EAC

Agenda

- Network Observability Objectives
- Are Enterprise Network Observability Objectives Different than those of Network Providers?
- Techniques, Methods and Tools
- Future
- Questions

Enterprise Objectives for Network Observability

- Provide optimal end user / application experience
    - Client and Server perspectives
- Identify issues ASAP
    - Preemptively if possible
- Assure environment is secure
    - Users, Networks, applications, platforms, data.
- Confirm regulatory, legal, corporate, contractual compliances
    - E.G. PCI, HIPAA, etc.

Are Network Observability Objectives Different Than Those of Network Providers?

- ISP’s need to assure packets get from A to B.
  - Typically higher packet rates and larger/more complex network topologies.
- Enterprises priorties are directed to optimize end to end QOE.
- Usually focus is on source and destination.
  - Performance and resource consumption – critical factors
- But many middle boxes/functons exist. **In both network ecosystems.**
  - E.G. Routers, Switches, LB’s, Firewall(S), Web Servers, App Servers, Auth Servers, DB’s / Clusters, Clouds, etc.
- All the above and more contribute to the QOE and must be monitored/managed.
- If issues exist, speedy triage is critical. ***

Techniques, Methods and Tools

- **Crucial to consolidate & correlate all pertinent data from all platforms (some we own)**
- Need to get all information to one central loction/application
- Convert to common formats and understand data relationships
- Partnerships with Network Providers can be effective!

- SNMP, Monitoring products, Security and Diagnostic Tools, Logs, Logs, Logs….
  - Convert all data to common format and consolidate, and correlate!
    - E.G. FW Rule (Block vs. Allowed) ---- effect on Client sessions
    - E.G. Storage or SAN latency and --- effect on DB & user response time
- When all else fails ……………. PACKET TRACES!
  - Collection & processing of this data is not easy or free – Visibility Networks.
  - Obtained information can be limited by increased levels of encryption. (TLS1.3).

- ALL THE ABOVE CAN BE COMPLEX, EXPENSIVE AND DIFFICULT TO OPERATE!

Hope For the Future?

- Build as much Network Observability into Standards and Protocols as possible!
  - PDM – RFC8250
- These types of approaches should be:
  - More accurate and meaningful.
  - Reslient to Security advancements
  - Less complex to deploy
  - Less overhead and cost!

What is most important to YOUR Enterprise?

Questions?

Reach out to Mike at:
mackermann@bcbsm.com

Thanks for attending!

Network Observability

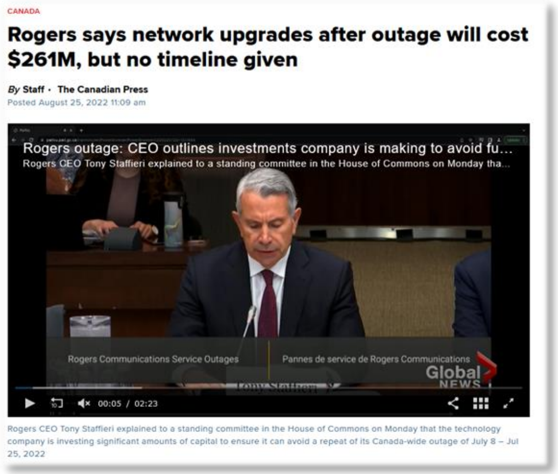
Service Provider Perspective

07.02.2024, Thomas Graf – thomas.graf@swisscom.com

Picture: Apollo 8, December 24th 1968

Nationwide Network Outages everywhere

Increasing in impact and duration - hinting Network Visibility deficiencies



CANADA

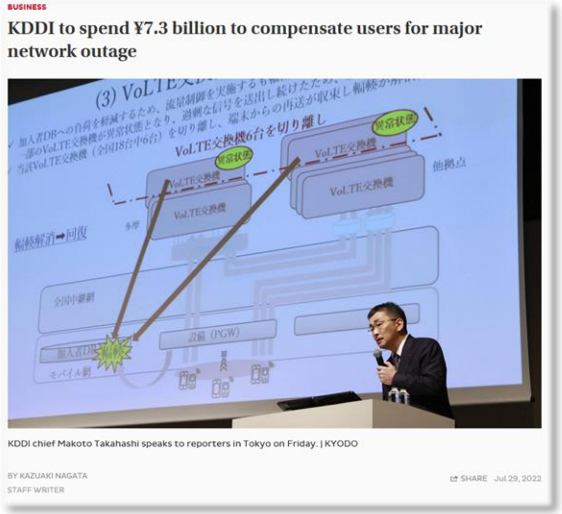
Rogers says network upgrades after outage will cost $261M, but no timeline given

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

Rogers 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
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 company is investing significant amounts of capital to ensure it can avoid a repeat of its Canada-wide outage of July 8 – Jul 25, 2022



BUSINESS

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
STAFF WRITER

SHARE Jul 29, 2022

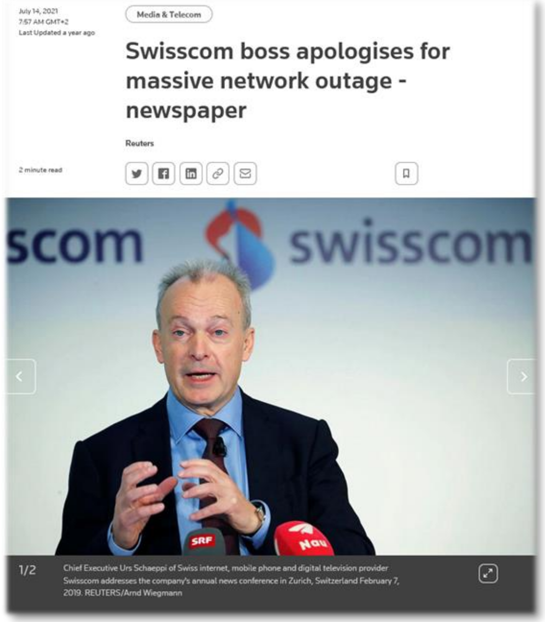
ORANGE FRANCE UNDER FIRE FOR MISHANDLING NETWORK OUTAGE

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

Optus: Telecom boss Kelly Bayer Rosmarin quits after Australian outage

6 days ago

The firm has come under fire following a nationwide network outage this month



July 14, 2021
7:57 AM GMT+2
Last Updated a year ago

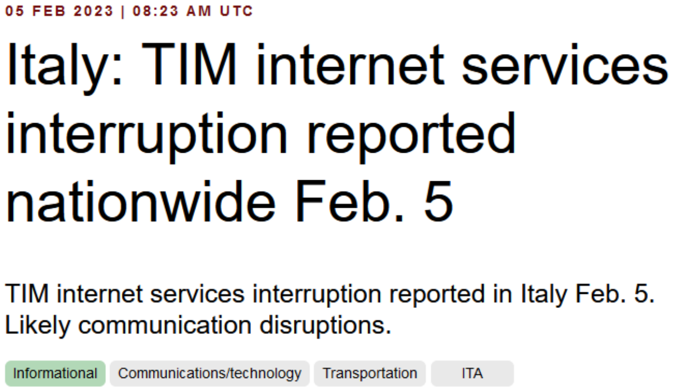
Media & Telecom

Swisscom boss apologises for massive network outage - newspaper

Reuters

2 minute read

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

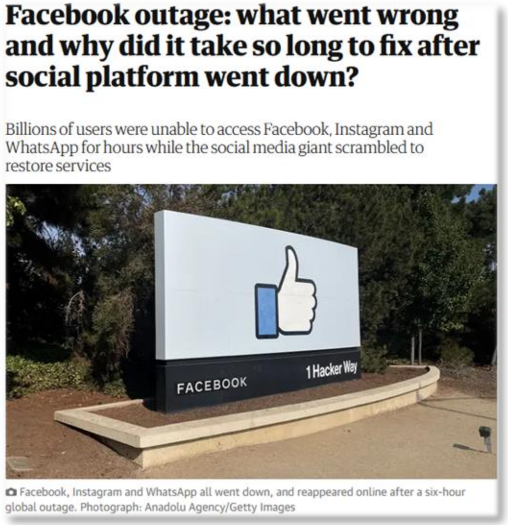


05 FEB 2023 | 08:23 AM UTC

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



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

“ It is our duty to recognize service interruption

before our customer does.

Why do we still often fail to be first ? “

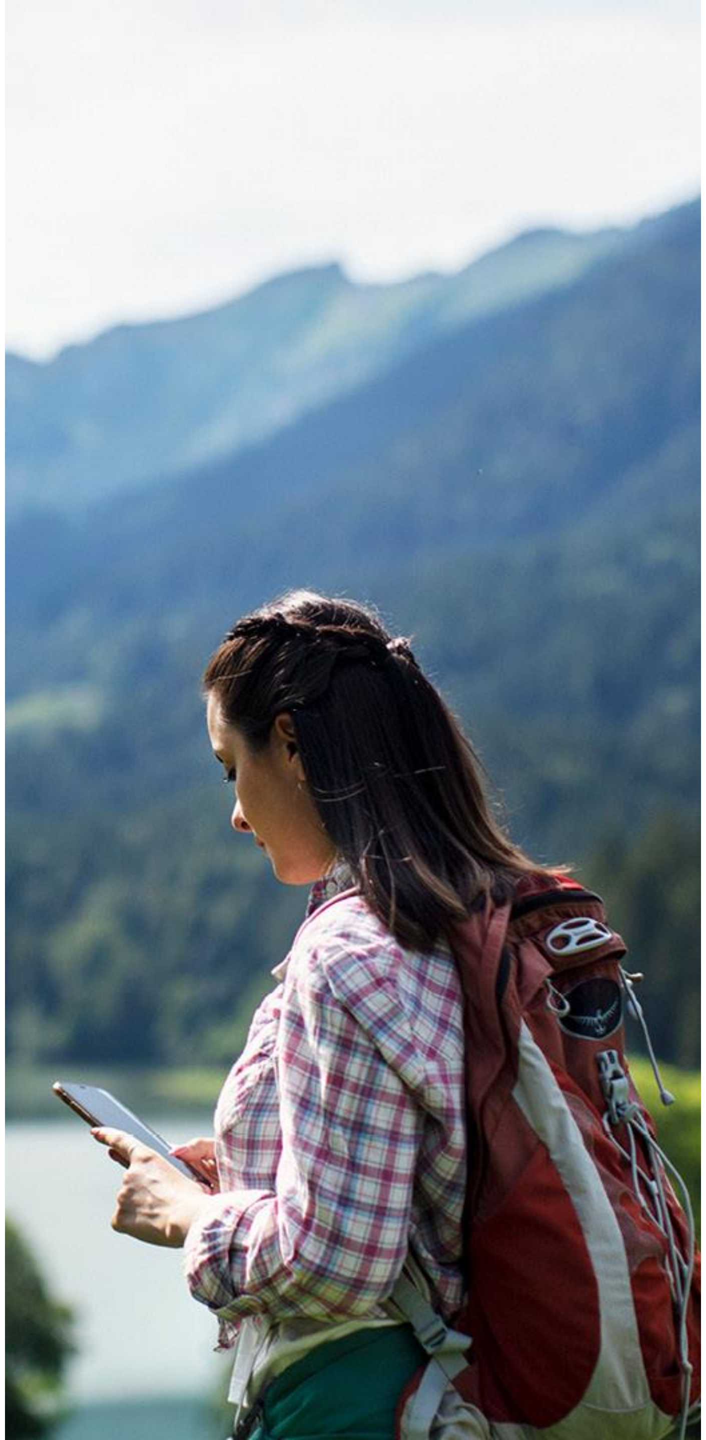
« At IETF only 9.85% of the activities are related to network automation and monitoring.

We are still using protocols designed 40 years ago to manage networks.

IP network protocols are not made to expose metrics for analytics. IPFIX and BGP monitoring protocol are the rare exception.

With the Network Management Operations (nmop) working group we bring operators needs to the IETF. »

Thomas Graf
Distinguished Network Engineer
and Network Analytics Architect at Swisscom



Pyramid of Technology

From envisioned to naturalized

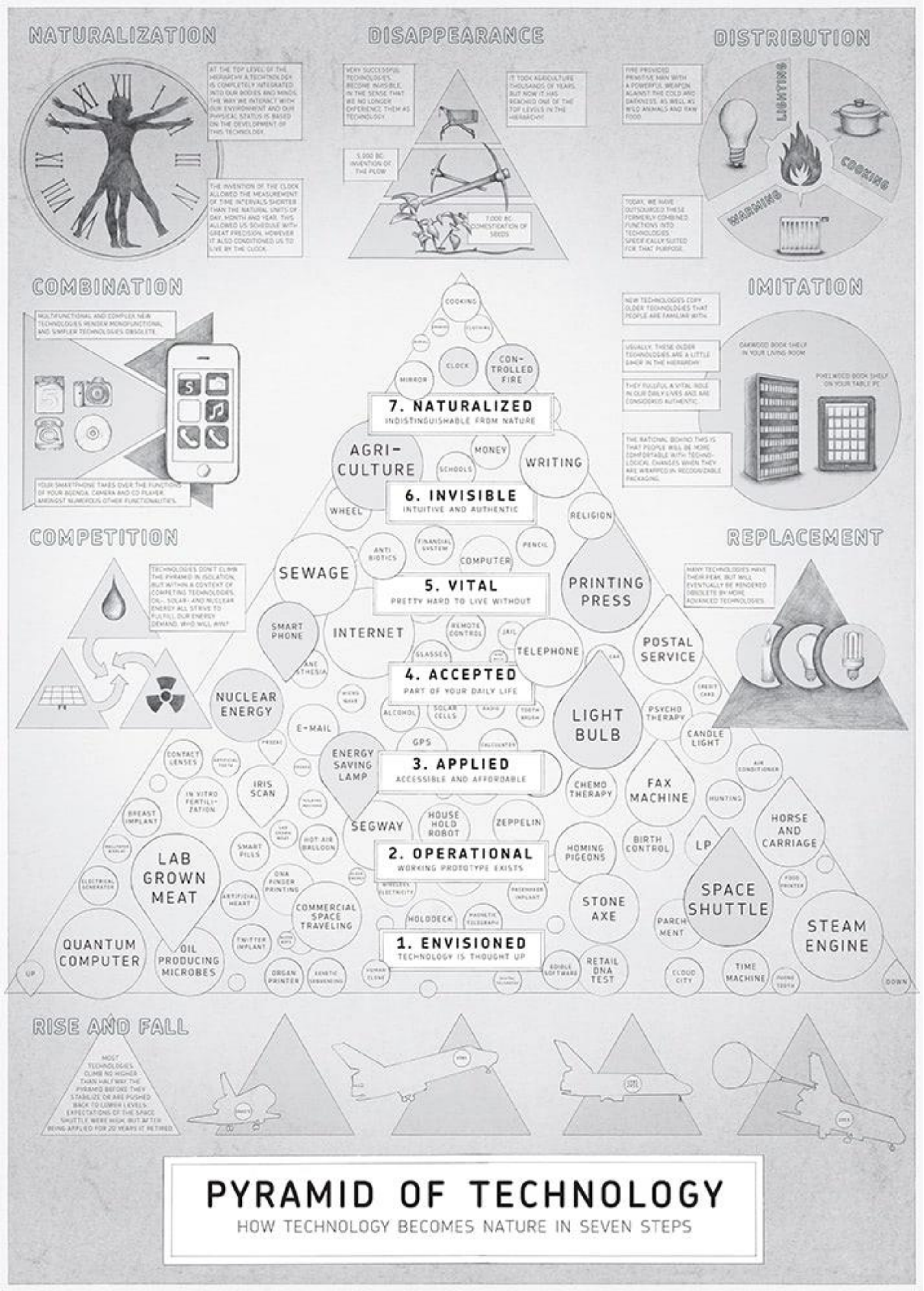
“ Every human being has to cope with technological change, yet few of us are aware of how new technologies are introduced, accepted and discarded in our society. The Pyramid of Technology visualizes how technology becomes nature in seven steps and what we can learn from that. It helps us to dream, build and live in our next nature — the nature caused by humans “

Analytical Use Cases are already traversing these technology stages at Swisscom as we defined the vision.

Pyramid of Technology
https://nextnature.net/projects/pyramid-of-technology

How technology becomes nature
https://www.youtube.com/watch?v=EXJB4Ync82c

The Idea Factory: Bell Labs and the Great Age of American Innovation
https://en.wikipedia.org/wiki/The_Idea_Factory



Network Analytics Use Cases

What they are and how they relate

Vital **Network Data Collection**

- Enables analytical use cases

Accepted **Verification, Troubleshooting and Notification**

- Dashboard, query and drill down on operational metrics

Operational **Network Anomaly Detection**

- State change for connectivity services

Envisioned **Network Service Level Indicator and Objective**

- State and state objective for connectivity services

Envisioned **Network Visualization**

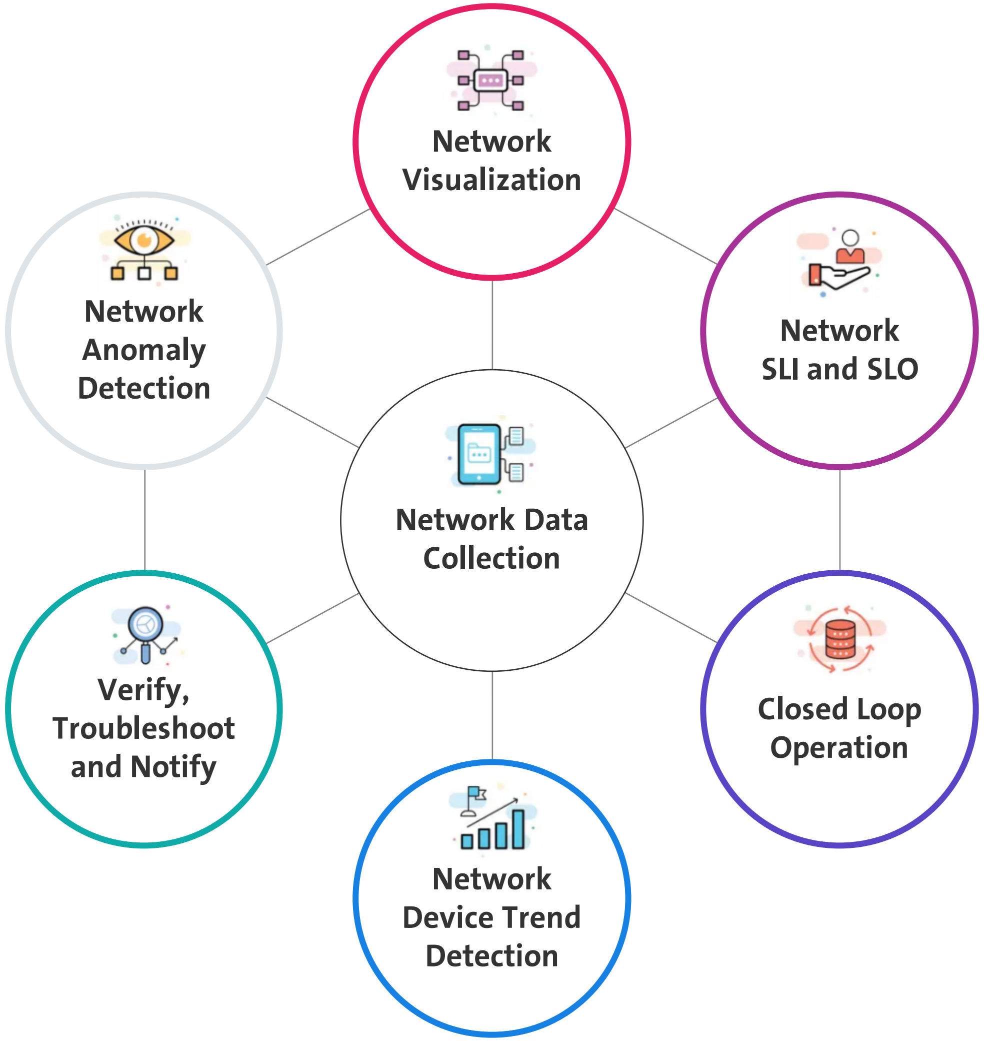
- Eases overview and access of metrics to humans

Envisioned **Network Device Trend Detection**

- Tracks and predicts critical devices resources

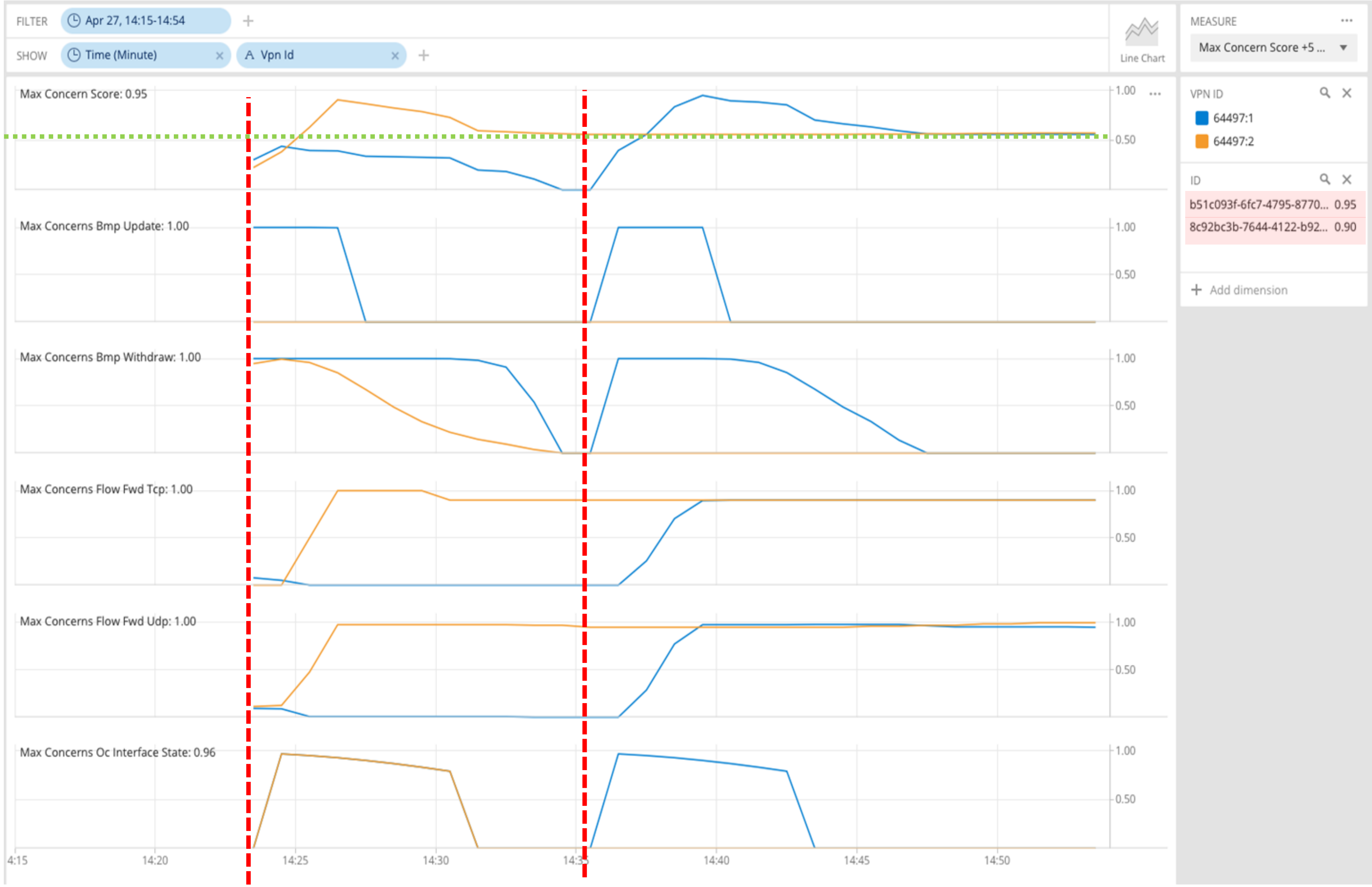
Envisioned **Closed Loop Operation**

- Automates network verification


Network Visualization
Network Anomaly Detection
Network SLI and SLO
Network Data Collection
Verify, Troubleshoot and Notify
Closed Loop Operation
Network Device Trend Detection

L3 VPN Network Anomaly Detection

Networks are deterministic – customers partially


FILTER: Apr 27, 14:15-14:54

SHOW: Time (Minute) | Vpn Id

MEASURE: Max Concern Score +5 ...

VPN ID
🟦 64497:1
🟧 64497:2

ID	
b51c093f-6fc7-4795-8770...	0.95
8c92bc3b-7644-4122-b92...	0.90

Line Chart
Add dimension
Max Concern Score: 0.95
Max Concerns Bmp Update: 1.00
Max Concerns Bmp Withdraw: 1.00
Max Concerns Flow Fwd Tcp: 1.00
Max Concerns Flow Fwd Udp: 1.00
Max Concerns Oc Interface State: 0.96
1.00
0.50
4:15
14:20
14:25
14:30
14:3
14:40
14:45
14:50

Analytical Perspectives

Monitors the network service and wherever it is congested or not.

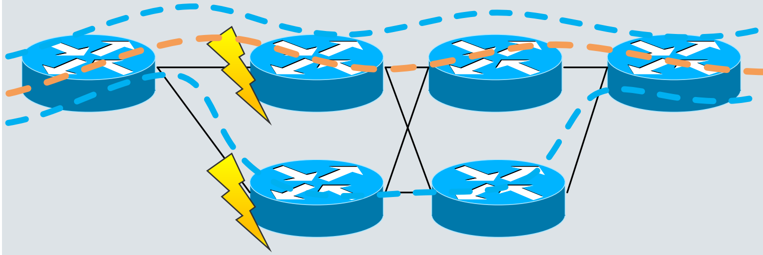
- BGP updates and withdrawals.
- UDP vs. TCP missing traffic.
- Interface state changes.
- Developed and refined in collaboration with the IETF community. Presented at the Applied Network Research Workshop 2023.

Network Events

1. VPN orange lost connectivity.
   VPN blue lost redundancy.
2. VPN blue lost connectivity.

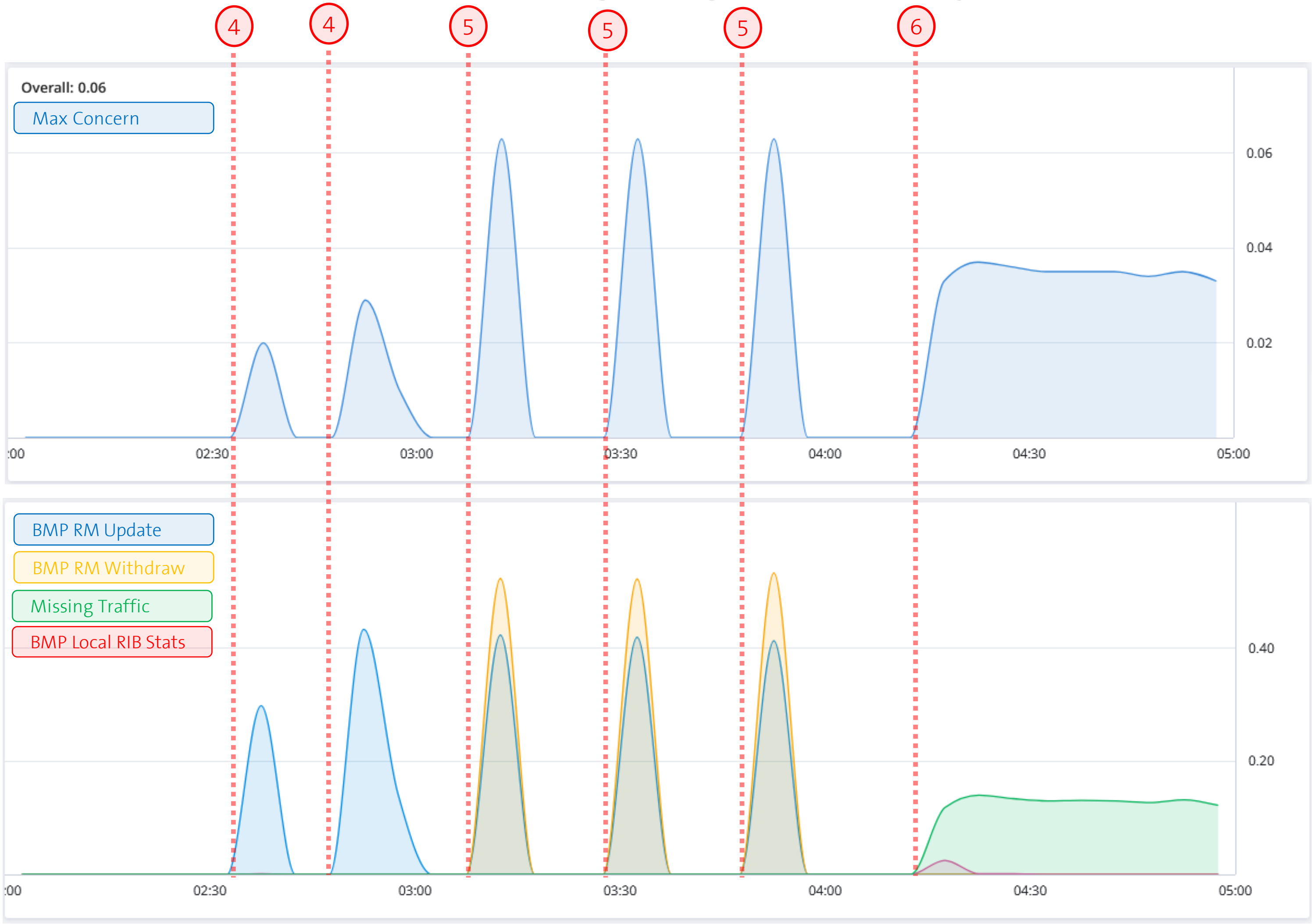
Key Point

- AI/ML **requires** network intent and network modelled data to deliver dependable results.



September 14th, Internet Access ASBR VRF Migration

64497:6304 (Mobile) - Bright Lights Anomaly Detection - **Live**



Max Concern Score: **0.06**
BMP RM update: **0.43**
BMP RM withdrawal: **0.53**
BMP Local RIB Stats: **0.03**

BMP route-monitoring Update/Withdraw check recognize topology change.

BMP Local RIB installed paths check recognized the path loss.

— BMP peer Down/Up check did not apply.

— Interface Down/Up check did not apply.

— Traffic Drop spike check did not apply.

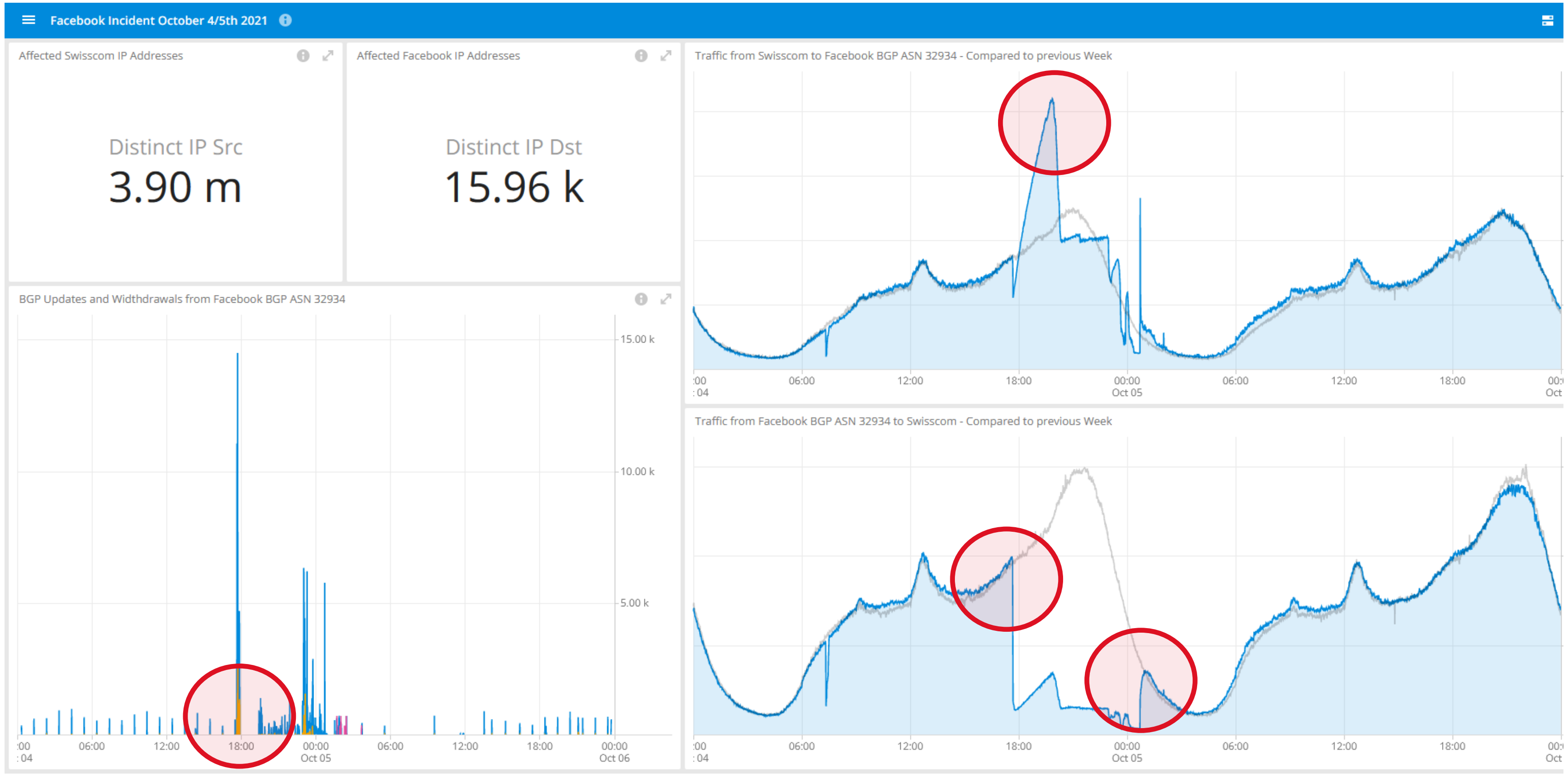
Missing Traffic check recognized the traffic decrease due to LC migration.

— Increased or decreased Flow Count did not apply.

Overall: 3 out of 7 checks have detected the routing topology change, where missing traffic was misleading. Works as designed.

Facebook Incident October 4/5th 2021

The Swisscom perspective



Facebook Incident October 4/5th 2021

Affected Swisscom IP Addresses

Distinct IP Src
3.90 m

Affected Facebook IP Addresses

Distinct IP Dst
15.96 k

Traffic from Swisscom to Facebook BGP ASN 32934 - Compared to previous Week

BGP Updates and Widthdrawals from Facebook BGP ASN 32934

Traffic from Facebook BGP ASN 32934 to Swisscom - Compared to previous Week

At 17:39 prefixes from Facebook BGP ASN 32934 where withdrawn. Outbound traffic steadily increased twofold until 20:20. Inbound traffic decreased by 85%.

Between 19:25 and 00:51, BGP updates and withdrawals where received.

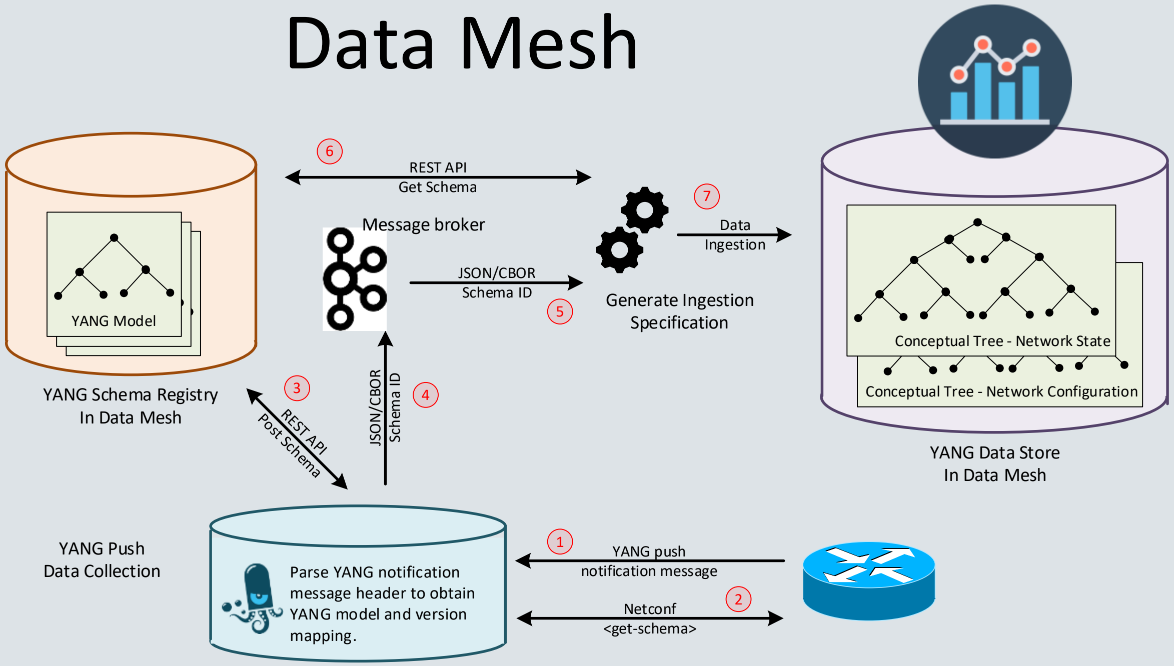
At 00:41 traffic rate restored to normal.

“ The solution comes with innovators.

That's why Swisscom cooperates at IETF with network operators, vendors and universities. “

When Big Data and Network become one

Marrying two messaging protocols



YANG is a data modelling language which will not only transform how we managed our networks; it will transform also how we manage our services.

News: 20 industry leading colleagues from 4 network operators, 2 network and 4 analytics providers, and 2 universities **commit on a project to integrate YANG and CBOR into data mesh. Next update IETF 119 Brisbane.**

Preserve YANG data module definition throughout the data processing chain. **Enable automated data correlation** among management, forwarding and control-plane **for Network Analytics use cases. Simplify** YANG push network data collection at high scale with low impact. **Suited for nowadays distributed forwarding systems. NMOP (Network Management Operations) Working Group at IETF.**

Yang
Kafka

IPFIX Covering Segment Routing

For MPLS-SR, SRv6 and On-path Delay

SRv6 is commonly standardized, network vendors implementations are available and network operators are at various stages in their deployments, missing data-plane visibility though.

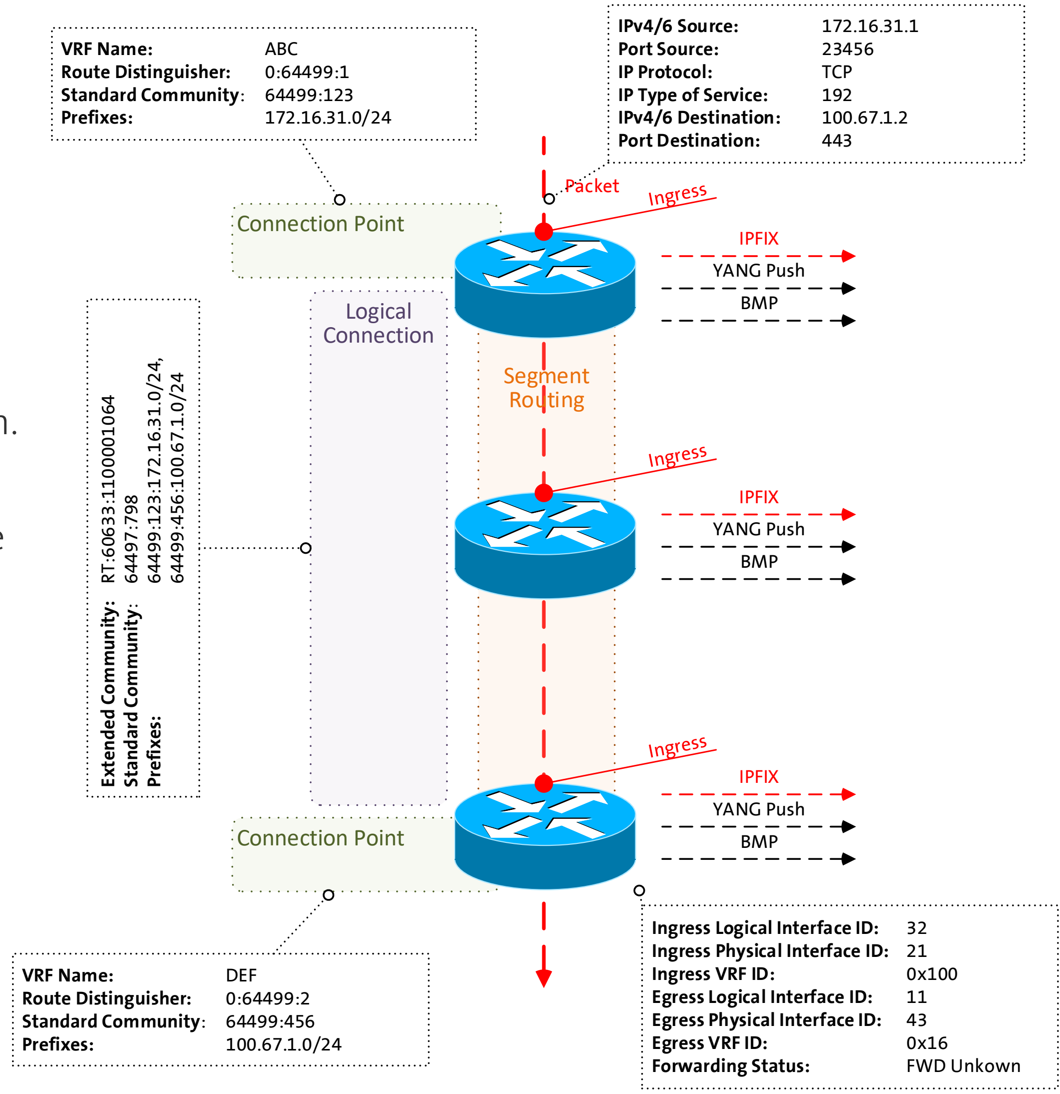
SRv6 coverage and On-Path Delay capabilities in IPFIX brings visibility for:

- Which routing protocol provided the label or IPv6 Segment in the SR domain.
- The active Segment where the packet is forwarded to in the SRv6 Domain.
- The Segment List where the packet is going to be forwarded throughout the SRv6 Domain.
- The Endpoint Behavior describing how the packet is being forwarded in the SRv6 Domain.
- The Min, Max and Average On-path delay at each hop in the SR domain.

Export of MPLS Segment Routing Label Type Information in IPFIX
https://datatracker.ietf.org/doc/html/rfc9160

Export of Segment Routing IPv6 Information in IPFIX
https://datatracker.ietf.org/doc/html/rfc9487

Export of Forwarding Path Delay in IPFIX
https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-ipfix-on-path-telemetry



VRF Name:	ABC
Route Distinguisher:	0:64499:1
Standard Community:	64499:123
Prefixes:	172.16.31.0/24

IPv4/6 Source:	172.16.31.1
Port Source:	23456
IP Protocol:	TCP
IP Type of Service:	192
IPv4/6 Destination:	100.67.1.2
Port Destination:	443

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

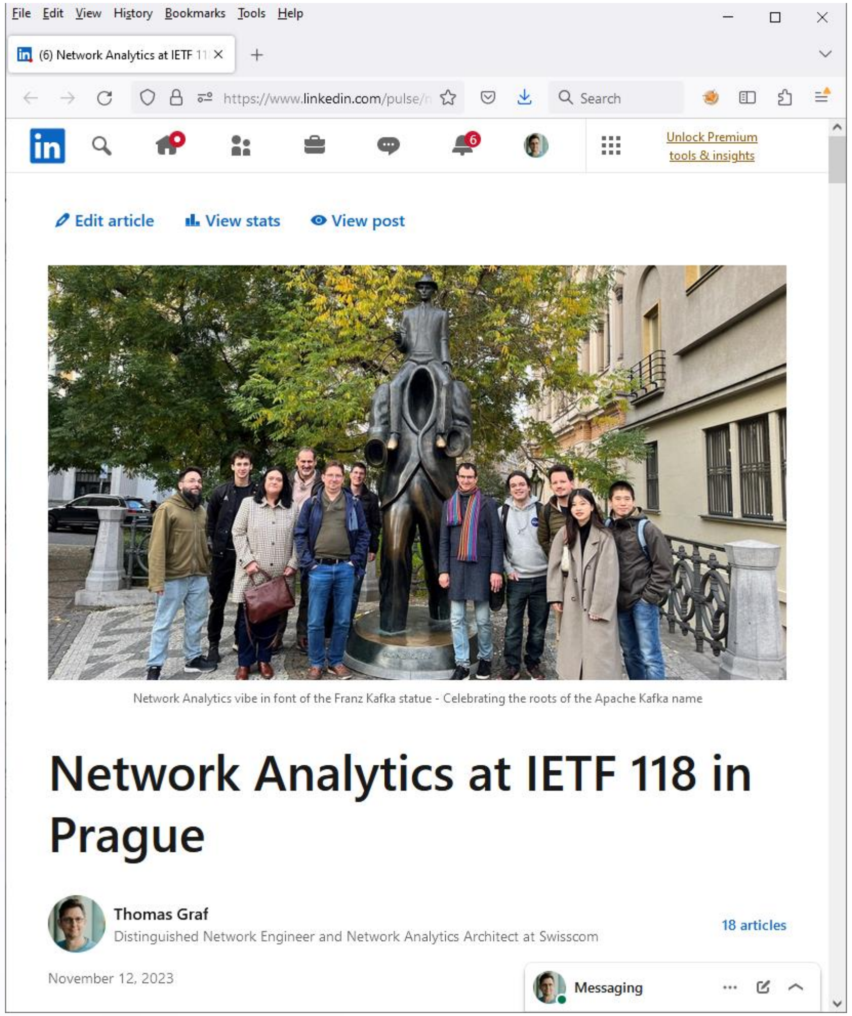
VRF Name:	DEF
Route Distinguisher:	0:64499:2
Standard Community:	64499:456
Prefixes:	100.67.1.0/24

Ingress Logical Interface ID:	32
Ingress Physical Interface ID:	21
Ingress VRF ID:	0x100
Egress Logical Interface ID:	11
Egress Physical Interface ID:	43
Egress VRF ID:	0x16
Forwarding Status:	FWD Unkown

Contact information

Swisscom
Daisy Network Analytics
Thomas Graf
Binzring 17
CH-8045 Zürich

thomas.graf@swisscom.com


File Edit View History Bookmarks Tools Help
(6) Network Analytics at IETF 11
https://www.linkedin.com/pulse/n
Search
in
6
Unlock Premium tools & insights
Edit article
View stats
View post
Messaging

Network Analytics vibe in front of the Franz Kafka statue - Celebrating the roots of the Apache Kafka name

Network Analytics at IETF 118 in Prague

Thomas Graf
Distinguished Network Engineer and Network Analytics Architect at Swisscom

18 articles

November 12, 2023

https://www.linkedin.com/pulse/network-analytics-ietf-118-prague-thomas-graf-2t82e/

Network Observability

A protocol design perspective

paolo@ntt.net

Observability in protocol / framework design

- Historically not a first class citizen in original designs
- With the issue fixed a-posteriori:
  - Let’s think for example to IPFIX, BMP
  - But not always .. DNS anybody?
- More recently there is increased consciousness:
  - Let’s think for example to SR
  - New issues: inter-operability a challenge sometimes

BMP (BGP Observability)

- Covers all key vantage points in a router BGP workflow
- Both real-time data streaming and event-driven covered
- Accurate timestamping
- Statistics
- Extraction of ancillary state data
- Use-cases:
  - Security
  - Troubleshooting & debugging
  - Correlation & closed-loop operations

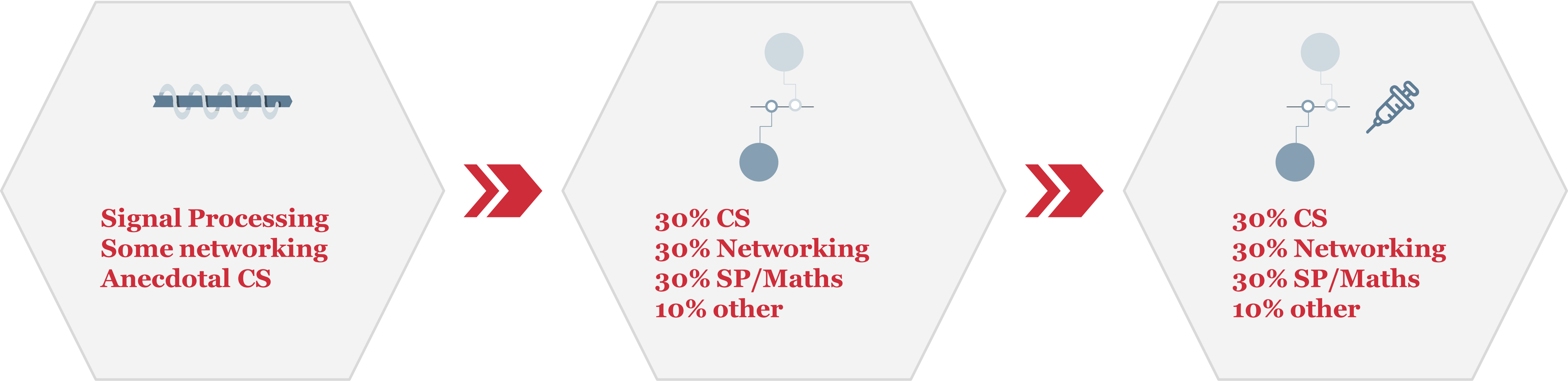
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Network Observability

Academic Perspective

Pierre.Francois@insa-lyon.fr

Evolution of the Telecom Eng. Student



Signal Processing
Some networking
Anecdotal CS

30% CS
30% Networking
30% SP/Maths
10% other

30% CS
30% Networking
30% SP/Maths
10% other

Telecom Engineers are CS engineers with a deep understanding of a network, using novel development tools….

Evolution of applied research topics in networking

Research based on a static view of an ISP network, typically focusing on a specific dimension

»

PoC Products analysing the network in near real-time, gathering an extremely large amount of data on a broad set of dimensions

Analytics Solutions should not be too taxing for the routers
Analytics Solutions should not be too costly to run

“ Network Management requires a

holistic network view

to act on operational or perform

configurational changes, manually or

automatically, as part of a closed loop action “