Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks

Alex HUANG FENG, INSA Lyon - alex.huang-feng@insa-lyon.fr

Pierre FRANCOIS, INSA Lyon - pierre.francois@insa-lyon.fr

Stéphane FRENOT, INSA Lyon - stephane.frenot@insa-lyon.fr

Thomas GRAF, Swisscom - thomas.graf@swisscom.com

Wanting DU, Swisscom - wanting.du@swisscom.com

Paolo LUCENTE, pmacct.net - paolo@pmacct.net

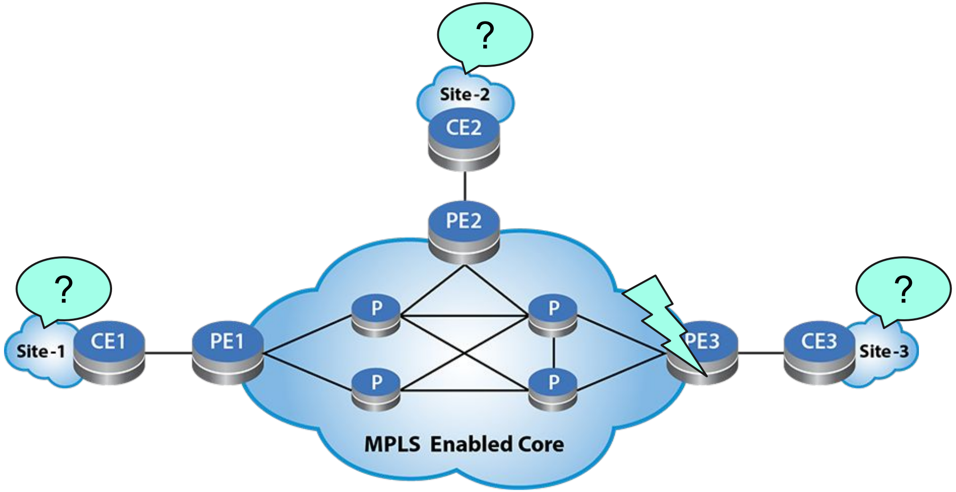
ANRW'23 - San Francisco

24/07/2023

Agenda

- Anomalies in BGP/MPLS and BGP/SRv6 VPN Networks
- Daisy Architecture
- IETF gaps
- Ongoing works

Anomalies in a BGP/MPLS and BGP/SRv6 VPN Networks



- An anomaly is an event occuring in the network that makes the customer unhappy
  - **Provider inflicted (incident)**
  - **Provider self-inflicted (upgrade)**
  - (Customer inflicted)

Internet outages on the News

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
00:03 / 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

25, 2022

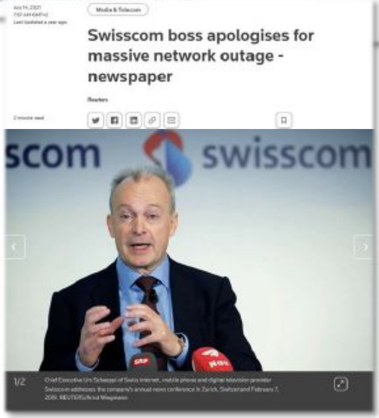
BUSINESS

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

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



July 14, 2021
7:53 AM GMT+2
Last Updated a year ago

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

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 restore services

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

Reasons to be good at detecting issues

- Issues happen to all networks
  - It’s how you deal with them that matter
- Service interruptions
  - make you look bad
  - cost you money
- Incident, **Detection**, ***Analysis***, Fix

Project

- Project funded by Swisscom
- Research and Open Source Development
  - Network information collection
    - Research
    - Standardisation
    - Implementation
  - Network measurements
    - Research
    - Standardisation
    - Implementation
  - Scalable Anomaly Detection Solution
    - Research
    - Implementation

Requirement 1

It needs to work !

Architecture Components

- Customer profiling
- Standard Data collection
- Correlation
- Anomaly detection
- Incident reporting

Architecture Components: Customer profiling (1)

- Customers differ in behavior
  - Flat vs Day/Night cycles
  - Customers with regular drops
- Profiles of similar behavior
  - Obtained with clustering
- Anomaly detection recipes based on profile

Architecture Components: Standard Data collection (2)

- Dimensions
  - Data-plane (IPFIX: RFC7011)
    - Traffic counters (5-tuple)
    - Packet drops
  - Control-plane (BMP: RFC7864)
    - BGP Update events
    - BGP Withdraw events
    - BGP Peer Down events
  - Management-plane (*YANG Push*: RFC8639, RFC8641)
    - Interface state changes
    - Interface counters

Architecture Components: Data correlation (3)

- Mapping Traffic counters to customer sites
    - IPFIX / BMP correlation
- Mapping interfaces to customers
    - IPFIX / YANG Push / BMP correlation

Architecture Components: Anomaly detection (4)

- For a Customer Profile,
  - we apply a set of independent strategies
  - NOC is alerted if one strategy detects an issue for the customer
- A strategy is one way to capture service health
  - e.g. “Did I just see a traffic collapse and BGP withdraws?”
  - Organized as a set of pipelines
- A pipeline is a sequence of conditionally executed checks
  - e.g. “Unusual customer traffic volume?”
    → “Check each customer site traffic levels”
- Checks are one dimensional observations
  - e.g. “Deviation from expected TCP traffic volume”
  - Define your own

Architecture Components: Incident reporting (5)

- When an alert is raised for a customer
  - Submit a ticket to the Network Operations Center (NOC)
  - Give the NOC details about the executed rules
    - Raw data
    - Details on the *checks*
- Permanent storage for replayability
  - What if scenarios
  - Experimenting with new strategies (bring your own)

IETF gap filling

- YANG push: Streaming large amounts of data from the router without stressing the router
  - draft-ietf-netconf-udp-notif-10
- New core network technology: SRv6
  - draft-ietf-opsawg-ipfix-srv6-srh-14
- New metrics: on-path delay
  - draft-ietf-opsawg-ipfix-on-path-telemetry-04

Other IETF Contributions

- YANG push:
  - draft-ahuang-netconf-notif-yang
  - draft-tgraf-netconf-notif-sequencing
  - draft-tgraf-yang-push-observation-time
  - draft-tgraf-netconf-yang-notifications-versioning
- On-path delay in iOAM DEX:
  - draft-ahuang-ippm-ioam-on-path-delay
  - draft-ahuang-ippm-dex-timestamp-ext

Ongoing works

- Analysis of real scenarios of onboarded customers in production (Swisscom)
  - 6 outages have been detected from real production data
    - 3 in real time
    - 3 in replay mode
- Exploration of new dimensions
  - anticipating vendor support
- The specific case of Internet Services
- Progressing with Standardization

Questions?

Alex HUANG FENG, INSA Lyon - alex.huang-feng@insa-lyon.fr

Pierre FRANCOIS, INSA Lyon - pierre.francois@insa-lyon.fr

Stéphane FRENOT, INSA Lyon - stephane.frenot@insa-lyon.fr

Thomas GRAF, Swisscom - thomas.graf@swisscom.com

Wanting DU, Swisscom - wanting.du@swisscom.com

Paolo LUCENTE, pmacct.net - paolo@pmacct.net