An Architecture for a Network Anomaly Detection Framework

draft-netana-nmop-network-anomaly-architecture-00

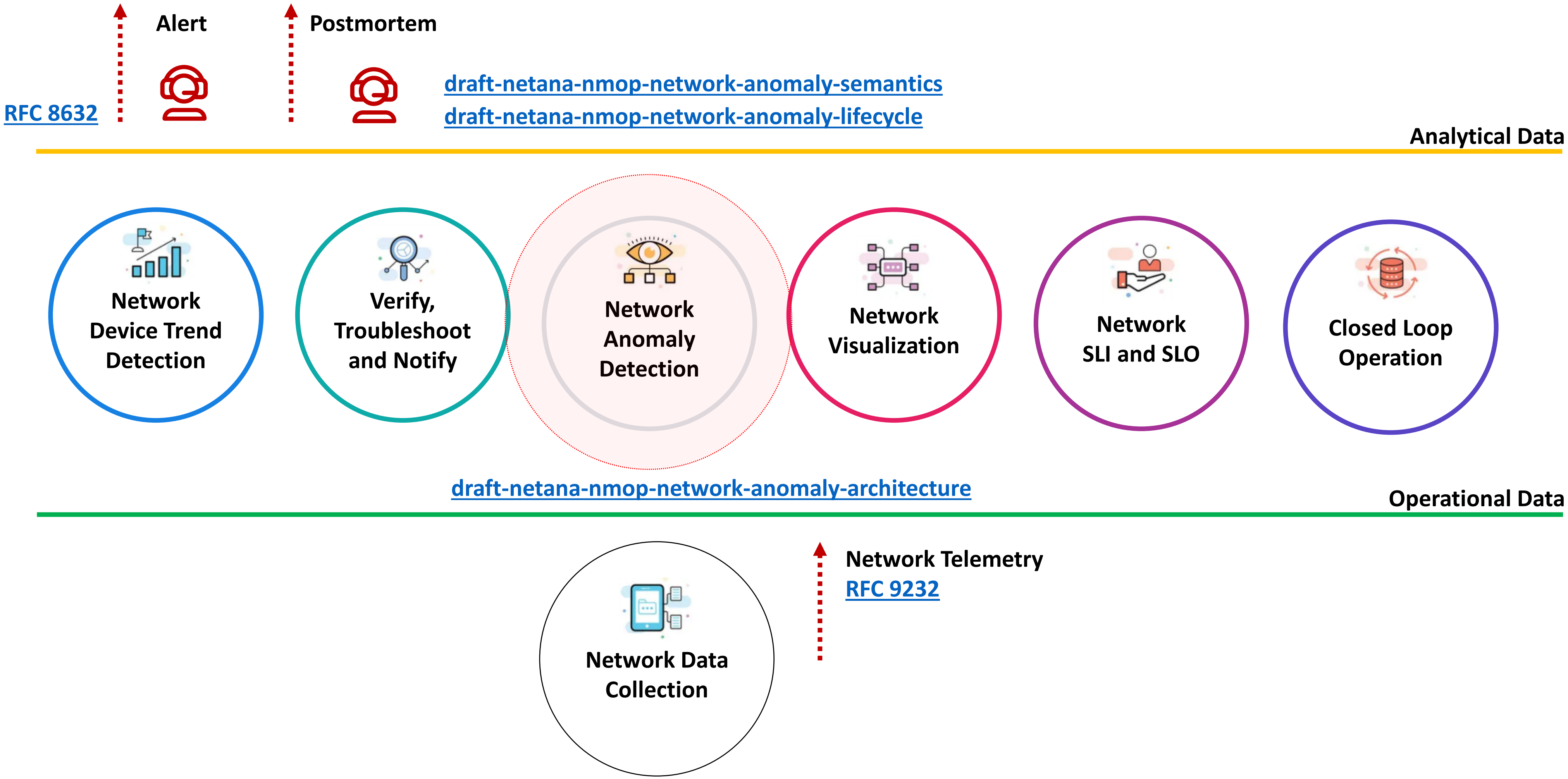
Motivation and architecture of a Network Anomaly Detection Framework
and the relationships to other documents describing
network symptom semantics and network incident lifecycle

wanting.du@swisscom.com
pierre.francois@insa-lyon.fr
thomas.graf@swisscom.com
vincenzo.riccobene@huawei-partners.com
alex.huang-feng@insa-lyon.fr

16. July 2024

Data Mesh organizes Data in Organizations

Enables Network Analytics use cases

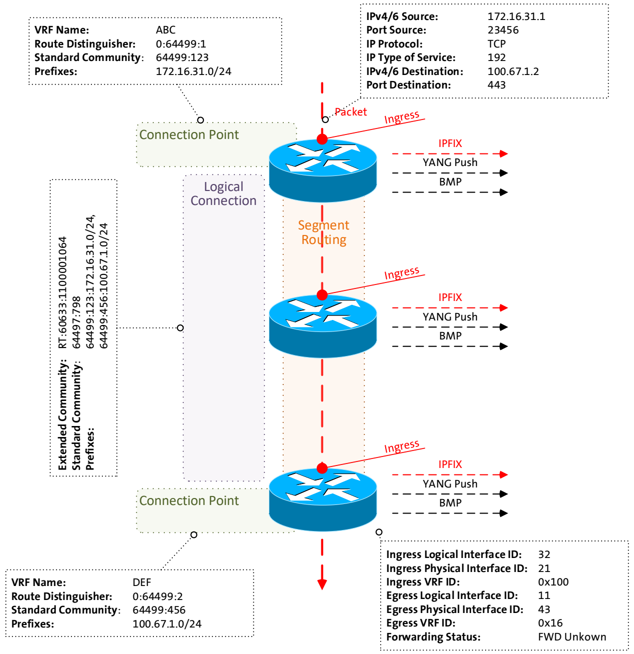


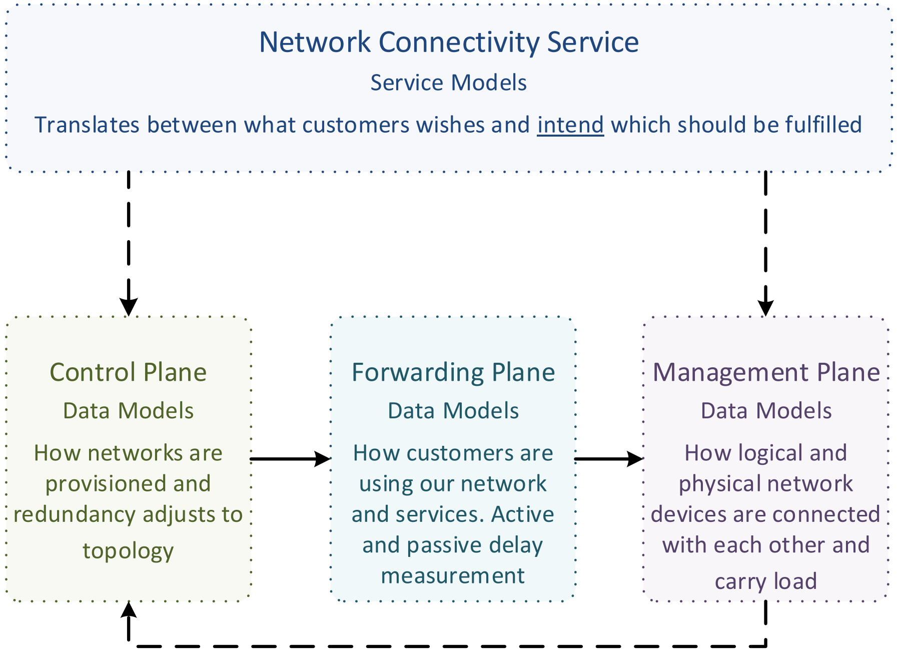
What to monitor

Which metrics are collected

« Network operators connect customers in routing tables called Connectivity Services »

« Network Telemetry (RFC 9232) describes how to collect data from all 3 network planes efficiently »





What does Network Anomaly Detection mean

Monitor changes, called outliers, in networks

Network Anomaly Detection

For Connectivity Services, Network Anomaly Detection **constantly monitors and detects any network or device topology change**, along with their associated forwarding consequences for customers as outliers. Notifications are sent to the Network Operation Center before the customer is aware of service disruptions. **It offers operational metrics for in-depth analysis,** allowing to understand in which platform the problem originates and facilitates problem resolution.

Answers

What changed and when, on which connectivity service, and how does it impact the customers?

Focuses

Provides meaningful connectivity service impact information before customer is aware of and support in root-cause analysis.

Data Mesh

Consumes operational real-time Forwarding Plane, Control Plane and Management Plane metrics and produces analytical alerts.

Direction

From connectivity service to network platform.

What our motivation is

Automate learn and improve

From network incidents postmortems we network operators **learn and improve** so does network anomaly detection and supervised and semi-supervised machine learning.

The more network incidents are observed, the more we can improve. With more incidents the **postmortem process needs be automated, let's get organized** first by defining human and machine-readable metadata semantics and annotate operational and analytical data.

Let's get further organized by exchanging standardized labeled network incident data among network operators, vendors and academia to **collaborate on academic research**.

« The community working on Network Anomaly Detection is probably the only group wishing for more network incidents »

Elements of the Architecture

```
        +---------+                     +--------------------+
        |Service  |                     |     Alert and      |
   |--- |Inventory|                     | Problem Management |
   |    |         |                     |       System       |
   |    +---------+                     +--------------------+
   |      |                                      ^     Stream
   |      |                                      |
   |      |       +---------+           +--------------------+
   |      |       | Post-   | Stream    |   Message Broker   |
   |      |       | mortem  | <-------- |  with Analytical   |
   |      |       | System  |           |    Network Data    |
   |      |       +---------+           +--------------------+
   |      |            |                         ^     Stream
   |      |            |                         |
   |      |            |                +--------------------+
   |      | Profile    | Fine           | Alert Aggregation  | Store Label
   |      | and        | Tune           | for Anomaly        | ------------|
   |      | Generate   | SDD            | Detection          |             |
   |      | SDD Config | Config         +--------------------+             |
   |      |            |                      ^  ^  ^ Stream               |
   |      v            v                      |  |  |                      ?
   |   +-------------------+            +--------------------+       +----------+
   |   | Service Disruption| Schedule   | Service Disruption | Replay |   Data   |
   |   |     Detection     | ---------->|     Detection      |<------ | Storage  |
   |   |   Configuration   | Detection  |                    |        |          |
   |   +-------------------+            +--------------------+        +----------+
   |                                      ^ ^ Stream ^ ^ ^                 ^
   |                                      | |        | | |                 |
   |                                    +----------+---------+             |
   |                                    | Network  |  Data   | Store       |
   |                                    |  Model   |  Aggr.  | ------------|
   |------------------------------->    |          | Process | Operational Data
                                        +----------+---------+
                                              ^  ^  ^ Stream
                                              |  |  |
                                        +--------------------+
                                        |   Message Broker   |
                                        |  with Operational  |
                                        |    Network Data    |
                                        +--------------------+
                                              ^  ^  ^ Stream
Subscribe                      Publish        |  |  |
          +--------------------+        +--------------------+
          | Network Node with  | ------>| Network Telemetry  |
--------->| Network Telemetry  | ------>|  Data Collection   |
          |    Subscription    | ------>|                    |
          +--------------------+        +--------------------+
```

- **Service Inventory** contains list of the connectivity services.
- **Service Disruption Detection** processes aggregated network data to decide whether a service is degraded or not.
- **Service Disruption Detection Configuration** defines the set of approaches that need to be applied to perform SDD.
- **Operational Data Collection** manages network telemetry subscriptions and transforms data into message broker.
- **Operational Data Aggregation** produces data upon which detection of a service disruption can be performed.
- **Network Modeling** establishes knowledge of network relationships.
- **Data Profiling** categorizes nondeterministic customer related data.
- **Detection Strategies** for a profile a detection strategy is defined.
- **Machine Learning** is commonly used to detect outliers or anomalies.
- **Storage** some algorithms may relay on historical (aggregated) operational data to detect anomalies.
- **Alerting** consolidates analytical insights and notifies.
- **Postmortem** refines and stores the network anomaly and symptom labels into the Label Store.
- **Replaying** to validate refined anomaly and symptom labels, historical operational data is replayed.

Semantic Metadata Annotation for Network Anomaly Detection

draft-netana-nmop-network-anomaly-semantics

```
module: ietf-symptom-semantic-metadata
  +--rw symptom
     +--rw id?                              yang:uuid
     +--rw event-id?                        yang:uuid
     +--rw description?                     string
     +--rw start-time?                      yang:date-and-time
     +--rw end-time?                        yang:date-and-time
     +--rw confidence-score?                score
     +--rw concern-score?                   score
     +--rw tags* [key]
     |  +--rw key       string
     |  +--rw value     string
     +--rw (pattern)?
     |  +--:(drop)
     |  |  +--rw drop                       empty
     |  +--:(spike)
     |  |  +--rw spike                      empty
     |  +--:(mean-shift)
     |  |  +--rw mean-shift                 empty
     |  +--:(seasonality-shift)
     |  |  +--rw seasonality-shift          empty
     |  +--:(trend)
     |  |  +--rw trend                      empty
     |  +--:(other)
     |     +--rw other                      string
     +--rw annotator
        +--rw (annotator-type)
        |  +--:(human)
        |  |  +--rw human           empty
        |  +--:(algorithm)
        |     +--rw algorithm       empty
        +--rw name?                 string
```

- **Symptom ID and description** uniquely identifies the detected anomaly. **Event ID, start/end-time and confidence/concern-score** uniquely identifies the network event with its start and end time, how confident the system identified the anomaly and how concerned an operator should be.
- **Tags** allows to add customer information.
- **Pattern** describes the identified pattern of the anomaly.
- **Annotator Name, Type,** describes wherever the anomaly was detected by a human or algorithm and uniquely identifies the system who/which detected.

Experiment: Network Anomaly Lifecycle

draft-netana-nmop-network-anomaly-lifecycle

« Network Anomaly Detection is an iterative process that requires continuous improvement »

```
4.  Lifecycle of a Network Anomaly

   The lifecycle of a network anomaly can be articulated in three
   phases, structured as a loop: Detection, Validation, Refinement.

                        +-------------+
              +-------> | Detection  | ---------+
  Adjustments |         +-------------+          | Symptoms
              |                                   |
              |                                   v
      +-------------+                     +-------------+
      | Refinement |<-------------------- | Validation |
      +-------------+                     +-------------+
                            Incident
                          Confirmation

          Figure 1: Anomaly Detection Refinement Lifecycle

   Each of these phases can either be performed by a network expert or
   an algorithm or complementing each other.
```

Detection: The Network Anomaly Detection stage is about the continuous monitoring of the network through Network Telemetry [RFC9232] and the identification of symptoms.

Validation: Decides if the detected symptoms are signaling a real incident or if they are to be treated as false positives.

Refinement: Network operator performs detailed postmortem analysis of the network incident, collected Network Telemetry data and detected anomaly with the objective to identify useful adjustments in the Network Telemetry data collection and Anomaly Detection system.

Experiment: Network Anomaly Lifecycle

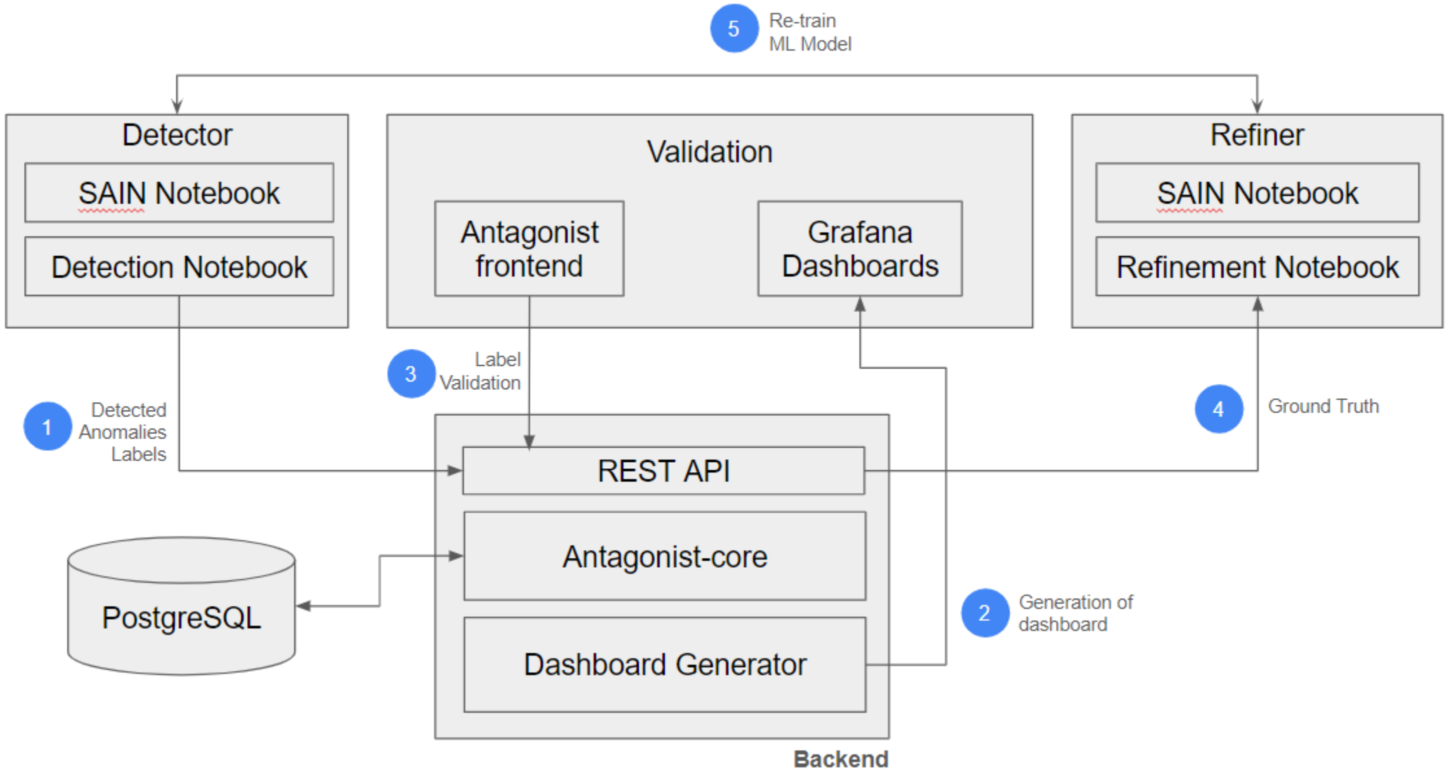
draft-netana-nmop-network-anomaly-lifecycle

```
module: ietf-network-anomaly-metadata
  +--rw network-anomalies
    +--rw network-anomaly* [id version]
      +--rw id               yang:uuid
      +--rw version          uint32
      +--rw description?     string
      +--rw state            identityref
      +--rw annotator
      |  +--rw (annotator-type)
      |  |  +--:(human)
      |  |  |  +--rw human          empty
      |  |  +--:(algorithm)
      |  |     +--rw algorithm      empty
      |  +--rw name?                empty
      +--rw symptoms* [symptom_id]
        +--rw symptom_id      yang:uuid
```

- **ID and Description** uniquely identifies the detected network anomaly (as a container of symptoms).
- **Description and State** provide general information regarding the anomaly and .
- **Annotator** describes the entity that observed the network anomaly: this can be a human or an algorithm (anomaly detection system).
- **Symptoms** provides a list of symptoms (based on ietf-symptom-metadata) that are part of this network anomaly.

Experiment: Antagonist

anomaly tagging on historical data



Next Steps:

- ➢ Improve scalability
- ➢ Validate with Swisscom Data

Goals:

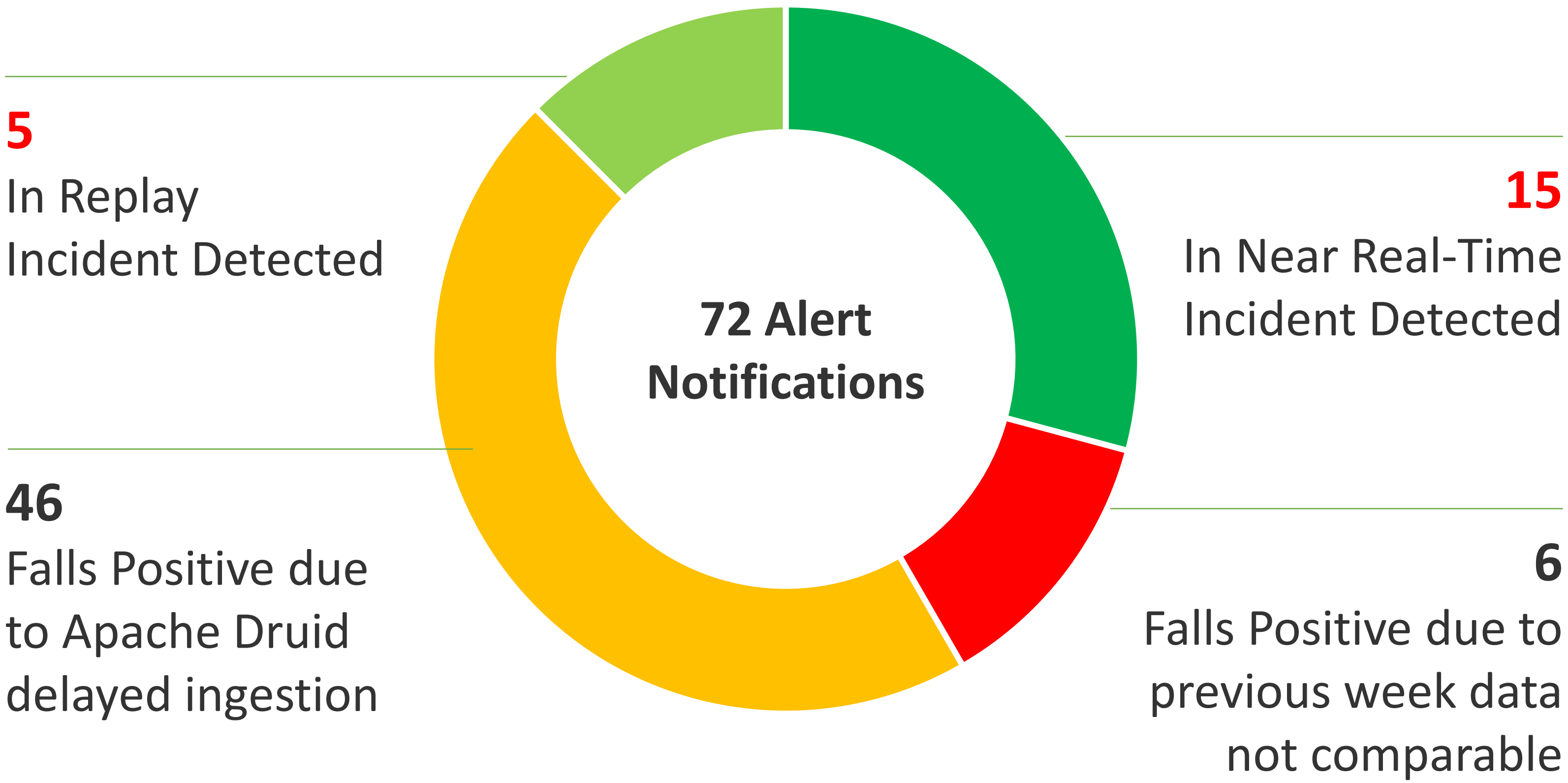
- ➢ Prove that YANG models contain all the necessary information
- ➢ Validate models across a wide range of use-cases
- ➢ Show interoperability between

Done so far:

- ✓ Validation with real operational data (Cloud monitoring)
- ✓ Validation with rule-based Network Anomaly Detector (SAIN RFC9417/RFC9418)
- ✓ Validation with a ML-based Network Anomaly Detector (Autoencoder)
- ✓ Add support for Re-training of ML-based models
- ✓ Add partial support for Metadata Filtering and search
- ✓ YANG model refinements to reflect the results of the coding
- ✓ Automatic dashboard generation

Swisscom - Cosmos Bright Lights PoC Summary

After 20 Incidents and 18 Months Time

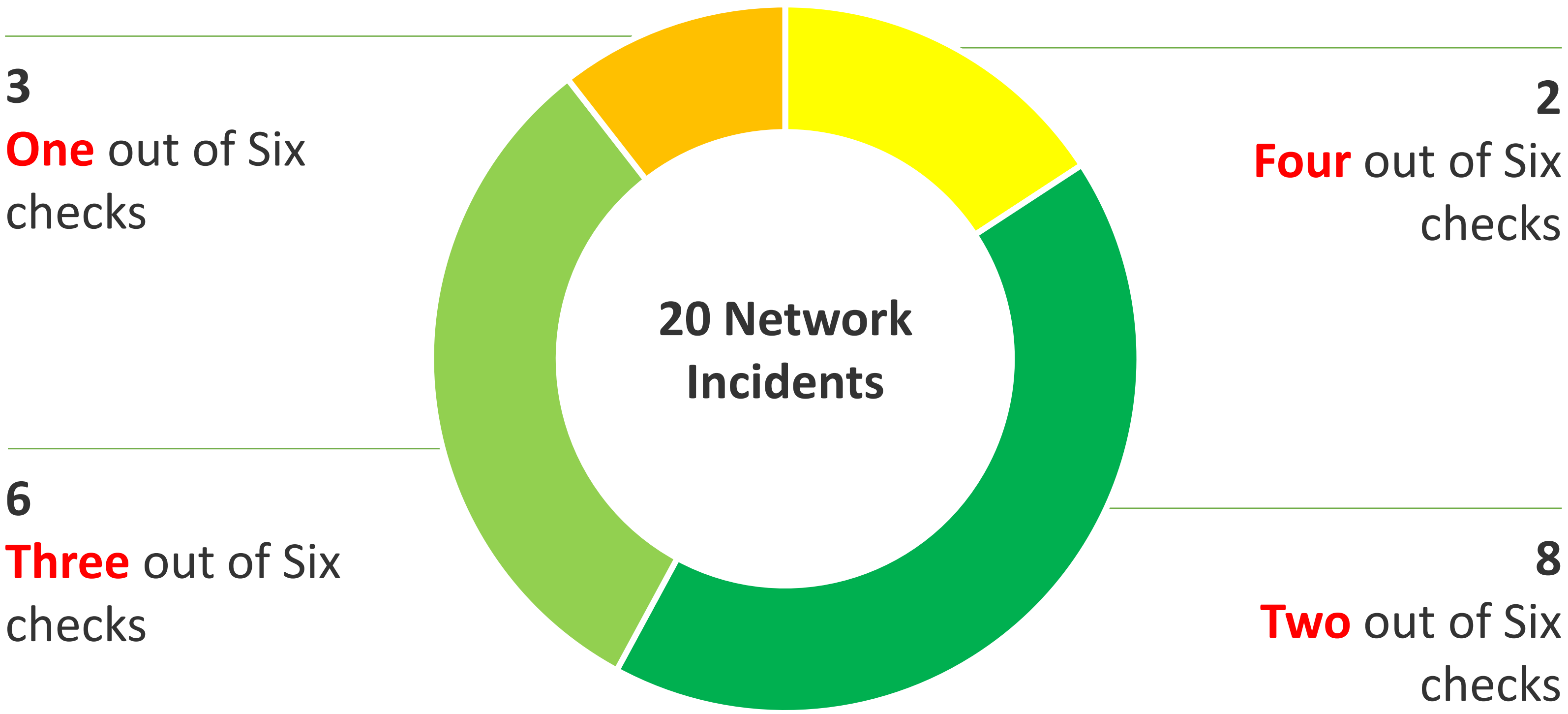


Key Facts in V0 (2023-2024)

- 16 L3 VPNs proactively monitored.
- Individual Service Disruption Detection rule accuracy is beyond 90%. Summed accuracy is beyond 95%.
- Max Concern score ranged between 0.06 and 0.85. In average 0.46.
- In 4 cases additional YANG, in 13 cases additional BMP, in 2 cases Netconf Transaction-ID and 1 case additional L2 IPFIX metrics would have helped to gain more visibility.
- Key observability feature missing: BMP Local RIB with Path Marking.

Swisscom - Cosmos Bright Lights PoC Detail

Multiple Perspectives increases Accuracy



Key Improvements in V1 (2024)

- >12000 L3 VPNs proactively monitored since June 2024.
- Realtime Streaming eliminates delayed ingestion falls positives and scaling.
- Improved profiling. Compares to multiple previous weeks and discard largest deviation eliminates falls positives.
  -> Work In progress

Key Improvements in V2 (2025)

- Annotate operational and analytical Network Incident data for reproduction.
- Enabling automated workflow. From PowerPoint slide decks to data driven actionable insights.

An Architecture for a Network Anomaly Detection Framework

Status, Summary and Next steps

Status of draft-netana-nmop-network-anomaly-architecture-00

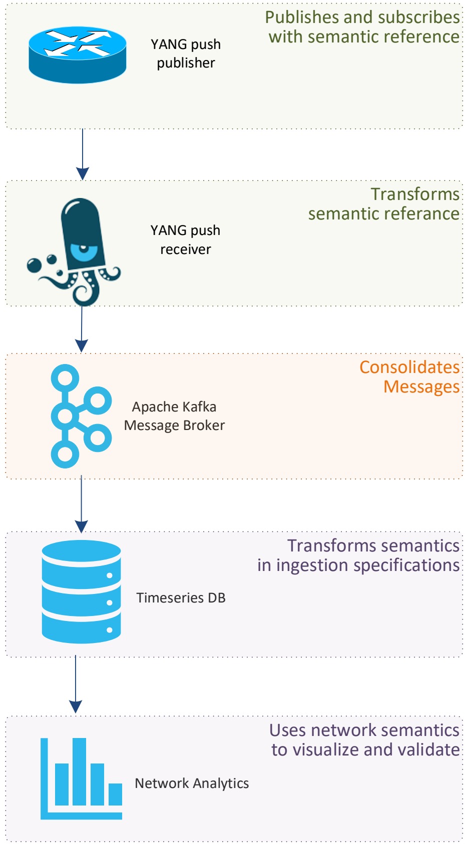
- Initial document published. Requesting feedback from the working group.

Status of draft-netana-nmop-network-anomaly-semantics-02 and draft-netana-nmop-network-anomaly-lifecycle-03

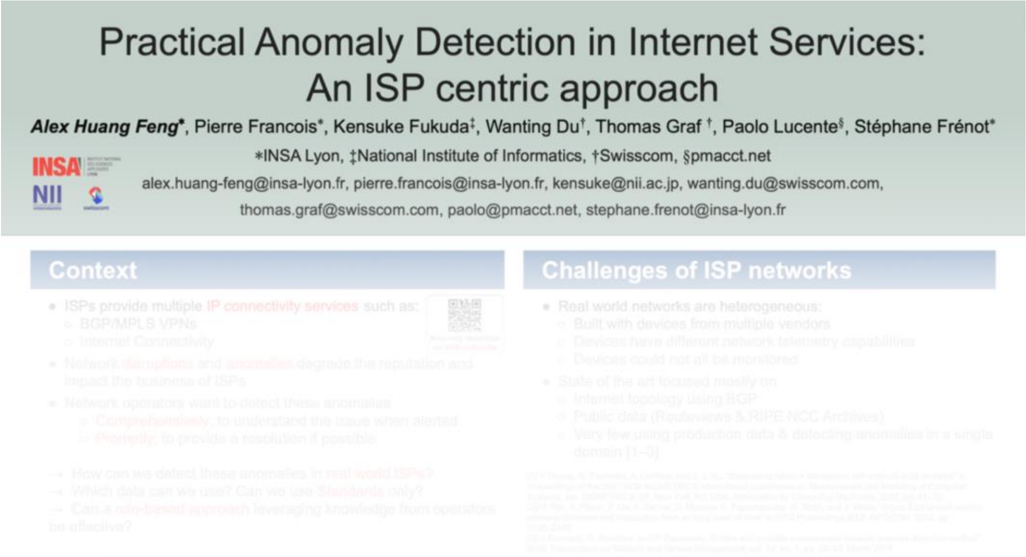
- Referred to draft-netana-nmop-network-anomaly-architecture as the architecture document.
- Change the term source to annotator and updated the YANG modules accordingly.
- Added/updated terminology section with references to draft-ietf-nmop-terminology and draft-netana-nmop-network-anomaly-architecture.
- Moved data mesh and outlier detection section to draft-netana-nmop-network-anomaly-architecture.

Next Steps

- ➢ **Request adoption for all 3 anomaly detection documents starting with draft-netana-nmop-network-anomaly-architecture-00.**
- ➢ **NMOP interim meeting on September 11th proposal**
  - ➢ **Network incident postmortem examples from Swisscom and Bell Canada**
  - ➢ **Detailing documents, updates and hackathon experiment results**



Relevant Papers for more Details



Practical Anomaly Detection in Internet Services: An ISP centric approach

*Alex Huang Feng**, Pierre Francois*, Kensuke Fukuda‡, Wanting Du†, Thomas Graf †, Paolo Lucente§, Stéphane Frénot*

*INSA Lyon, ‡National Institute of Informatics, †Swisscom, §pmacct.net

alex.huang-feng@insa-lyon.fr, pierre.francois@insa-lyon.fr, kensuke@nii.ac.jp, wanting.du@swisscom.com, thomas.graf@swisscom.com, paolo@pmacct.net, stephane.frenot@insa-lyon.fr

Context

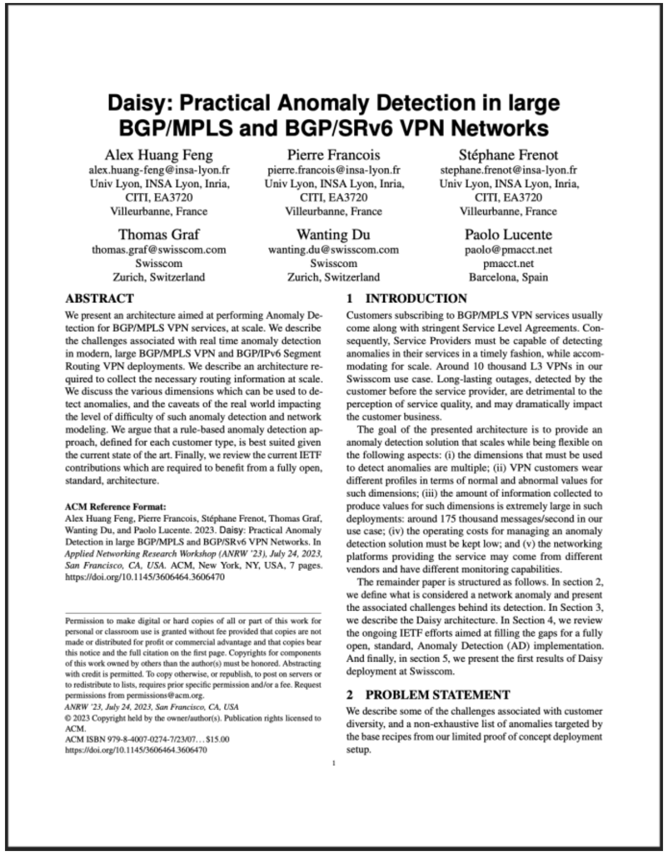
- ISPs provide multiple IP connectivity services such as:
  - BGP/MPLS VPNs
  - Internet Connectivity
- Network disruptions and anomalies degrade the reputation and impact the business of ISPs
- Network operators want to detect these anomalies
  - Comprehensively: to understand the issue when alerted
  - Promptly: to provide a resolution if possible

→ How can we detect these anomalies in real world ISPs?
→ Which data can we use? Can we use Standards only?
→ Can a rule-based approach leveraging knowledge from operators be effective?

Challenges of ISP networks

- Real world networks are heterogeneous:
  - Built with devices from multiple vendors
  - Devices have different network telemetry capabilities
  - Devices could not all be monitored
- State of the art focused mostly on
  - Internet topology using BGP
  - Public data (Routeviews & RIPE NCC Archives)
  - Very few using production data & detecting anomalies in a single domain [1–3]

Paper "**Practical Anomaly Detection in Internet Services: An ISP centric approach**"
accepted at AnNet'24
(in conjunction with IEEE NOMS'24)
Seoul, Korea (6–10 May 2024)
[Will be presented as a poster the May 6th 2024]



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

Alex Huang Feng, alex.huang-feng@insa-lyon.fr, Univ Lyon, INSA Lyon, Inria, CITI, EA3720, Villeurbanne, France
Pierre Francois, pierre.francois@insa-lyon.fr, Univ Lyon, INSA Lyon, Inria, CITI, EA3720, Villeurbanne, France
Stéphane Frenot, stephane.frenot@insa-lyon.fr, Univ Lyon, INSA Lyon, Inria, CITI, EA3720, Villeurbanne, France
Thomas Graf, thomas.graf@swisscom.com, Swisscom, Zurich, Switzerland
Wanting Du, wanting.du@swisscom.com, Swisscom, Zurich, Switzerland
Paolo Lucente, paolo@pmacct.net, pmacct.net, Barcelona, Spain

ABSTRACT

We present an architecture aimed at performing Anomaly Detection for BGP/MPLS VPN services, at scale. We describe the challenges associated with real time anomaly detection in modern, large BGP/MPLS VPN and BGP/IPv6 Segment Routing VPN deployments. We describe an architecture required to collect the necessary routing information at scale. We discuss the various dimensions which can be used to detect anomalies, and the caveats of the real world impacting the level of difficulty of such anomaly detection and network modeling. We argue that a rule-based anomaly detection approach, defined for each customer type, is best suited given the current state of the art. Finally, we review the current IETF contributions which are required to benefit from a fully open, standard, architecture.

ACM Reference Format:
Alex Huang Feng, Pierre Francois, Stéphane Frenot, Thomas Graf, Wanting Du, and Paolo Lucente. 2023. Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks. In *Applied Networking Research Workshop (ANRW '23), July 24, 2023, San Francisco, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3606464.3606470

ACM ISBN 979-8-4007-0274-7/23/07…$15.00
https://doi.org/10.1145/3606464.3606470

1 INTRODUCTION

Customers subscribing to BGP/MPLS VPN services usually come along with stringent Service Level Agreements. Consequently, Service Providers must be capable of detecting anomalies in their services in a timely fashion, while accommodating for scale. Around 10 thousand L3 VPNs in our Swisscom use case. Long-lasting outages, detected by the customer before the service provider, are detrimental to the perception of service quality, and may dramatically impact the customer business.

The goal of the presented architecture is to provide an anomaly detection solution that scales while being flexible on the following aspects: (i) the dimensions that must be used to detect anomalies are multiple; (ii) VPN customers wear different profiles in terms of normal and abnormal values for such dimensions; (iii) the amount of information collected to produce values for such dimensions is extremely large in such deployments: around 175 thousand messages/second in our use case; (iv) the operating costs for managing an anomaly detection solution must be kept low; and (v) the networking platforms providing the service may come from different vendors and have different monitoring capabilities.

The remainder paper is structured as follows. In section 2, we define what is considered a network anomaly and present the associated challenges behind its detection. In Section 3, we describe the Daisy architecture. In Section 4, we review the ongoing IETF efforts aimed at filling the gaps for a fully open, standard, Anomaly Detection (AD) implementation. And finally, in section 5, we present the first results of Daisy deployment at Swisscom.

2 PROBLEM STATEMENT

We describe some of the challenges associated with customer diversity, and a non-exhaustive list of anomalies targeted by the base recipes from our limited proof of concept deployment setup.

1

Paper "**Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks**"
published at ACM/IRTF ANRW'23
San Francisco, USA (24 July 2023)
Open access: http://hal.science/hal-04307611