An Architecture for a Network Anomaly Detection Framework

draft-ietf-nmop-network-anomaly-architecture-01

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

03. November 2024

Open questions from Anomaly Detection Interim Meeting

1. Is it worth to document lessons learned/shared out of this valuable « bring your own outage » (credits to Rob :-)) effort? Share Quick Wins?
2. Is the WG interested to investigate means that would help with auto-generation of correlation and then help with efficient mitigation? Do we have a candidate technical approach? Can data annotations be useful here?
3. Call for contributions to the KG experiment with a focus on anomaly
   - Share more lessons on automatic mapping of YANG to ontologies?
4. We have so far two drafts to “plug” in the network anomaly detection framework
   - Do they fulfill the needs expressed so far?
   - Do we need others?

Problem Statement and Motivation

How it is being addressed in which document

Network Anomaly Detection

When operational or configurational changes in connectivity services are happening, the objective is to detect interruption at network operation faster than the users using those connectivity services

In order to achieve this objective, automation in network monitoring is required. This automation needs to monitor network changes holistically by monitoring all 3 network planes simultaneously and detect whether that change is service disruptive.

Through network incidents postmortems we network operators learn and improve so does network anomaly detection and supervised and semi-supervised machine learning. With more and more incidents the postmortem process demands automation and with the standardization of labeled network incident collaboration among network operators, vendors and academia is facilitated.

- draft-ietf-nmop-network-anomaly-architecture describes the motivation and architecture and the relationship to other two documents.
- draft-netana-nmop-network-anomaly-semantics defines Symptom semantics to enable standardized data exchange to validate results with network engineers and improve supervised and semi-supervised machine learning systems.
- draft-netana-nmop-network-anomaly-lifecycle describes on managing the lifecycle process, in order to facilitate network engineers to interact with the network anomaly detection system to refine the detection abilities over time.

An Architecture for a Network Anomaly Detection Framework

Status and Next steps

Deployment Status

- Cosmos Bright Lights streaming based implementation deployed in Swisscom production environment. Service auto profiling successfully deployed. Monitoring >12'000 L3 VPN's.
- Bell Canada data processing chain is operational. Preparations for deployment started.

Deployment Next Steps

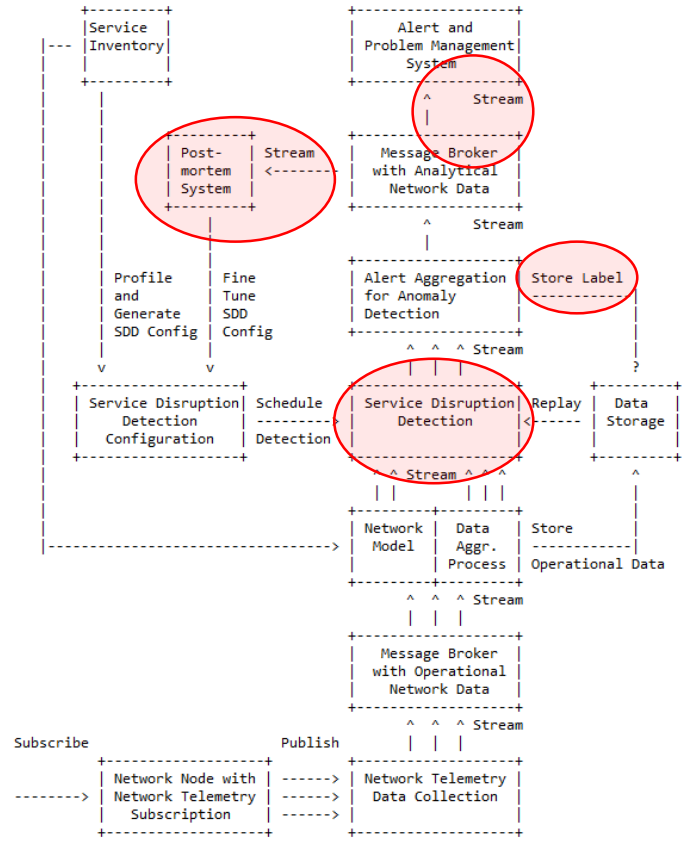
- Preparing code for Bell Canada deployment. Code refactoring according to latest annotation and notification semantics.
- Continue search for other network operators interested in collaboration and co-development.

Document Status

- Knowledge Graph references for rule in section 2.3 and symptom definitions in section 2.4.2 were added as per request from Nacho.
- Merged editorial updates from Qin in section 1.2.
- Merged terminology input from Adrian in regard to "network topology state" vs. "network state", "alert" vs. "alarm" and "component" vs. "resource" to be aligned with draft-ietf-nmop-terminology.

Document Next Steps

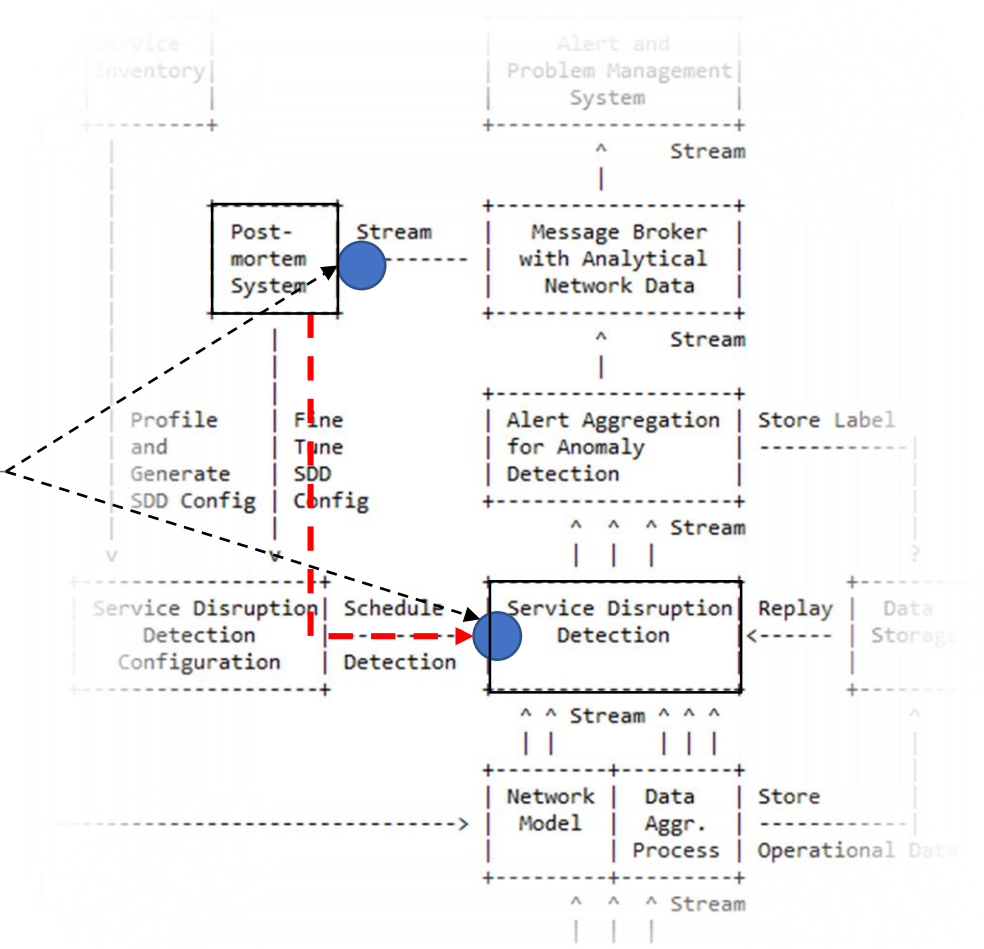
- **-> Incorporate already received feedback from Michael and look forward for feedback from Nacho on Knowledge Graph related changes.**
- **-> Looking forward for review and feedback from working group.**



Relationship between Service Disruption Detection and Post-mortem

draft-netana-nmop-network-anomaly-semantics

draft-netana-nmop-network-anomaly-lifecycle



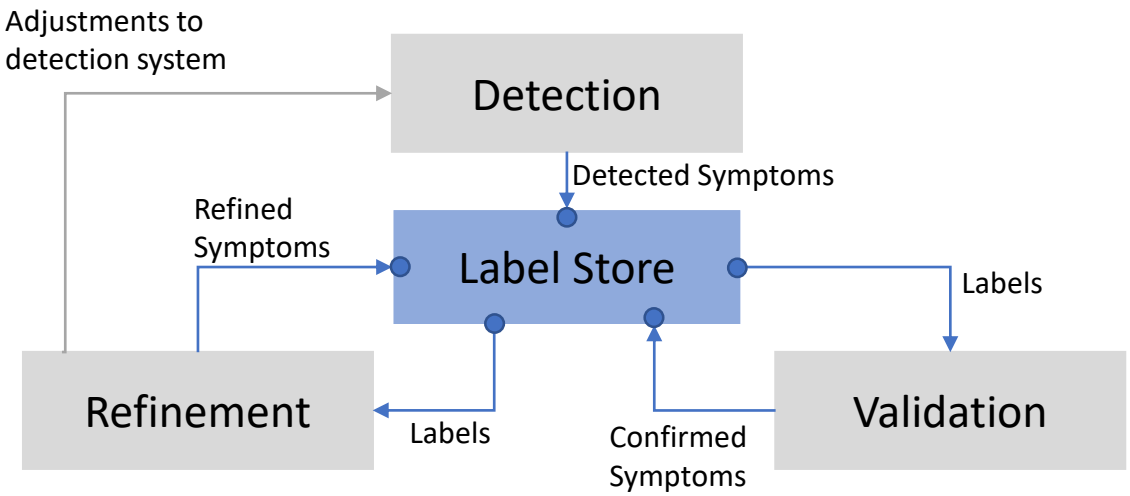
Service Disruption System: System consuming operational data and performing disruption detection
Post-mortem: process to improve the Service Disruption Detection System adding learnings from past disruptions

Network Anomaly Lifecycle and Anomaly Semantic

draft-netana-nmop-network-anomaly-lifecycle & draft-netana-nmop-network-anomaly-semantics

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

- The approach proposed in these documents is the introduction of a **Label Store for network anomaly detection**
- It addresses **two main challenges** in the network anomaly detection domain:
  - The **creation of labelled datasets** to train and evaluate anomaly detection algorithms and technologies
  - The **support for the human-in-the-loop paradigm** for what concerns the automated anomaly detection process.



- **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 operators perform postmortem analysis of incidents, analyze the telemetry data and detected anomalies with the objective to identify useful adjustments in the data collection and Anomaly Detection system.

The document proposes a standardization of the API of the Label Store

Semantic Metadata Annotation and Anomaly Lifecycle

Status and Next steps

Document Status

- Merged terminology input from Adrian "alert" vs. "alarm" and "occurrence"
- Embraced comment from Lionel on making the lifecycle data model self-contained
- Introduce a clearer cut of scope between the two drafts:
  - The **Lifecycle data model** now defines the “relevant-state” as a collection of generic anomalies (and it contains all the related fields, (like start / end time, confidence-score, concern-score)
  - The **semantic data model** provides a specific augmentation of the lifecycle in relation to the semantic of symptoms for connectivity services according to RFC9232.
- Updated the draft according to the comments from Med, sent on the mailing list.
- Updated YANG module with relevant-state container and notification augmentations to enable a structured and extensible YANG module tree.
  -> See next slides for details.

Deployment Status

- Antagonist PoC at IETF 121 hackathon, https://github.com/vriccobene/antagonist
  -> See NMOP presentation in the afternoon’s slot.

Semantic Metadata Annotation and Anomaly Lifecycle

Symptom Data Model

```
module: ietf-network-anomaly-symptom-cbl

+--rw symptom!
     |  +--rw smcblsymptom:action?          string
     |  +--rw smcblsymptom:reason?          string
     |  +--rw smcblsymptom:cause?           string
     |  +--rw (smcblsymptom:plane)?
     |     +--:(smcblsymptom:forwarding)
     |     |  +--rw smcblsymptom:forwarding?   empty
     |     +--:(smcblsymptom:control)
     |     |  +--rw smcblsymptom:control?     empty
     |     +--:(smcblsymptom:management)
     |        +--rw smcblsymptom:management?   empty
```

Service Data Model

```
module: ietf-network-anomaly-symptom-cbl

+--rw service!
     +--rw id       yang:uuid
     +--rw smtopology:vpn-service-container
     |  +--rw smtopology:vpn-service* [vpn-id]
     |     +--rw smtopology:vpn-id     string
     |     +--rw smtopology:vpn-name?   string
     |     +--rw smtopology:site-ids*   string
     +--rw smtopology:vpn-node-termination-container
        +--rw smtopology:vpn-node-termination* [hostname route-distinguisher]
           +--rw smtopology:hostname            inet:host
           +--rw smtopology:route-distinguisher    string
           +--rw smtopology:peer-ip*
           |     inet:ip-address
           +--rw smtopology:next-hop*
           |     inet:ip-address
           +--rw smtopology:interface-id*        int32
```

Symptom Semantic Metadata draft

augmentation

Relevant State Data Model

```
module: ietf-relevant-state
+--rw relevant-state
   +--rw id  yang:uuid
   +--rw description?    string
   +--rw start-time      yang:date-and-time
   +--rw end-time?       yang:date-and-time
   +--rw anomalies* [id version]
      +--rw id       yang:uuid
      +--rw version      yang:counter32
      +--rw state        identityref
      +--rw description?  string
      +--rw start-time    yang:date-and-time
      +--rw end-time?     yang:date-and-time
      +--rw confidence-score          score
      +--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 name     string
      |  +--rw (annotator-type)?
      |     +--:(human)
      |     |  +--rw human?          empty
      |     +--:(algorithm)
      |        +--rw algorithm?     empty
      +--rw symptom!
      |  +--rw id          yang:uuid
      |  +--rw concern-score          score
      +--rw service!
        +--rw id         yang:uuid
```

Network Anomaly Lifecycle draft

Next Steps

draft-netana-nmop-network-anomaly-lifecycle

- Integration with Swisscom Lab
- Explore validation of these models with other operators

draft-netana-nmop-network-anomaly-semantics

- Discussion with authors **draft-havel-nmop-digital-map** to identify proper ways to structure service-topology augmenting the right IETF models.
  - Explored documents: RFC 8299, RFC 9182, RFC 9181, RFC 8343, RFC 8345, RFC 9375, draft-ietf-idr-bgp-model

Discussion Points

draft-netana-nmop-network-anomaly-lifecycle

- Any feedback on the new structure of the model?
- Is this draft the right place where to define the “relevant-state”?

draft-netana-nmop-network-anomaly-semantics

- Any feedback on the new structure of the Symptom and the Service metadata and the separation between documents?

- We would like to request adoption

Thanks!