An Architecture for a Network Anomaly Detection Framework

draft-ietf-nmop-network-anomaly-architecture-00

Status update and next steps

wanting.du@swisscom.com
pierre.francois@insa-lyon.fr
thomas.graf@swisscom.com

11. September 2024

Why This I-D?

A Reminder

- This document describes motivation and a generic and extensible architecture of a Network Anomaly Detection Framework.
- Anchors draft-netana-nmop-network-anomaly-semantics and draft-netana-nmop-network-anomaly-lifecycle documents.
- Different applications will be described and exampled with open-source running code.

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.

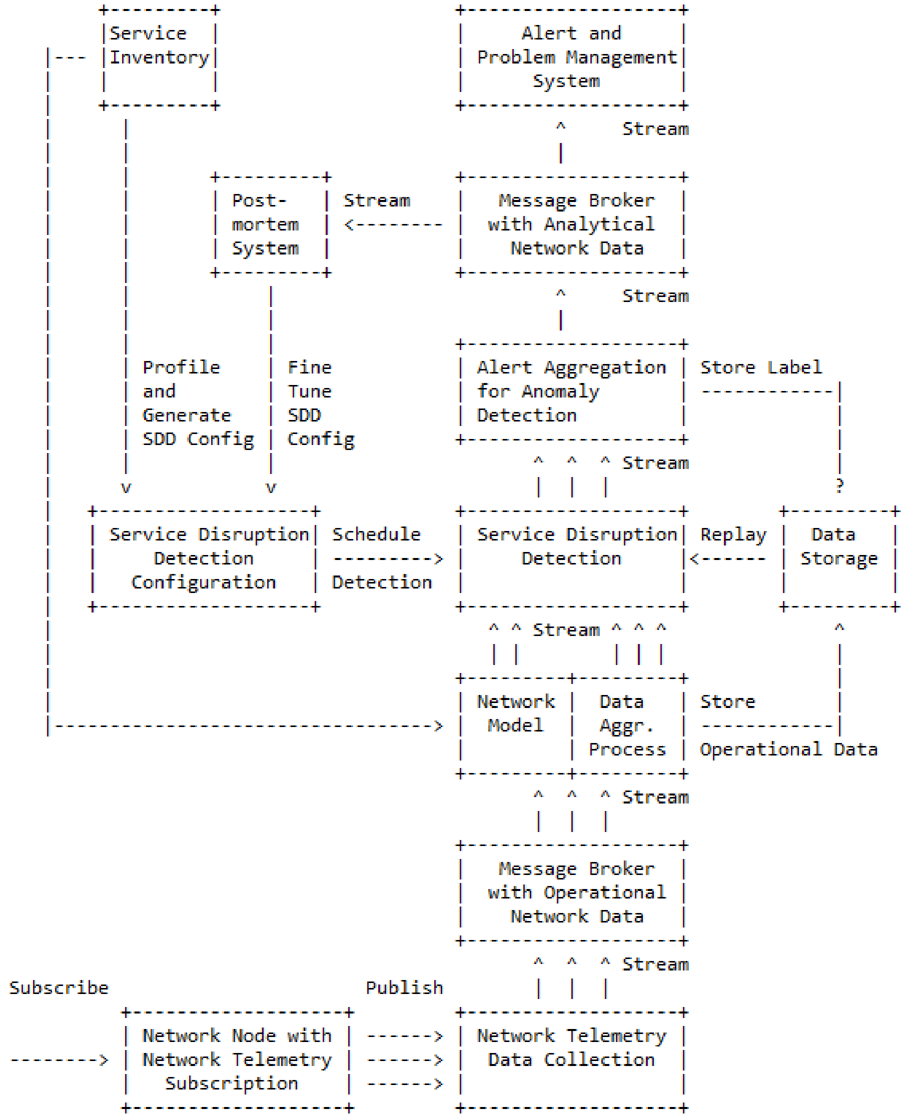
Data Mesh

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

Direction

From connectivity service to network platform.

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.

An Architecture for a Network Anomaly Detection Framework

Status, Open issues and Next steps

Status of draft-ietf-nmop-network-anomaly-architecture

- Reference document to anchor anomaly detection work items.
- Working group adopted. Thanks Alex and Nacho for feedback.

Open issues and feedback

- Optimize document structure
- Detail architecture elements
- References suggestion:
  - [draft-marcas-nmop-knowledge-graph-yang]
  - [draft-tailhardat-nmop-incident-management-noria-01]
  - [draft-mackey-nmop-kg-for-netops]
  - [draft-netana-nmop-network-anomaly-semantics]
  - [RFC9232]

- **Terminology consolidation**
  - Service VS Customer
  - Symptom

Next Steps

➢ **Update draft-ietf-nmop-network-anomaly-architecture to address working group comments**