An Architecture for a Network Anomaly Detection Framework

draft-ietf-nmop-network-anomaly-architecture-07
draft-ietf-nmop-network-anomaly-semantics-05
draft-ietf-nmop-network-anomaly-lifecycle-05

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

Problem Statement and Motivation

How it is being addressed in each document

Network Anomaly Detection

To **detect service interruptions** before users do, network operations must use **automated**, **holistic** monitoring across all **three network planes**.

- draft-ietf-nmop-network-anomaly-architecture describes the **motivation**, **architecture** and the **relationship** to other two documents.

By **standardizing labeled incident data** and **automating the postmortem process**, operators can **improve machine learning** models continuously and **foster better collaboration** between vendors and academia.

- draft-ietf-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-ietf-nmop-network-anomaly-lifecycle describes the lifecycle process, enabling network engineers to **interact** with the network anomaly detection system to **refine the detection abilities** over time.

Network Anomaly Detection Architecture

DRAFT-IETF-NMOP-NETWORK-ANOMALY-ARCHITECTURE-07

Network Anomaly Detection Architecture

Document summary

Motivation:

Human-driven troubleshooting does not scale due to the growing number of dependencies

Approach:

This draft defines a standardized, architecture-level framework

Outcome:

Enable automated service disruption detection

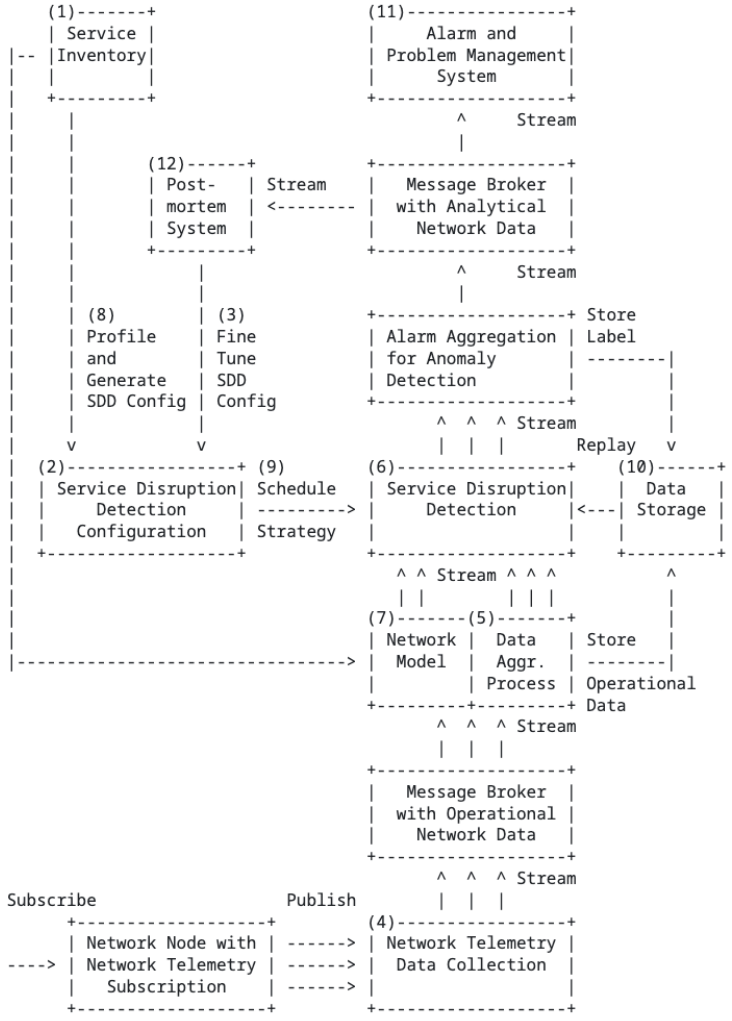


Figure 1: Service Disruption Detection System Architecture

draft-ietf-nmop-network-anomaly-architecture

Network Anomaly Detection Architecture

Key draft updates since v-05

- **Terminology update**
  - Change from “customer profile” to “service profile” to ensure consistency across reference documentation (RFC 8969).
  - Added formal “Rules" definition to distinguish between knowledge-based approach and ML approach.
- **Restructure**
  - Reorganisation Service Disruption Section to improve reading
- **Refinement**
  - Clarified the relationship between Semantic, Rule, & Knowledge-based detection.
  - Refined definition: collective outlier, confidence score, concern score.
  - Refined clarification: Alarm-raising criteria, Data storage considerations, Operational data aggregation
- Explicitly **out-scoped** Service Degradation based on WG review feedback

Network Anomaly Detection Architecture

Document implementation and operational experience

L3 VPN – Real-Time Incident Analysis

Swisscom TV service was severely impaired during 6 hours due to hardware faults and a software defect, which together led to a DoS condition.


PANORAMA

Abonnieren

Login

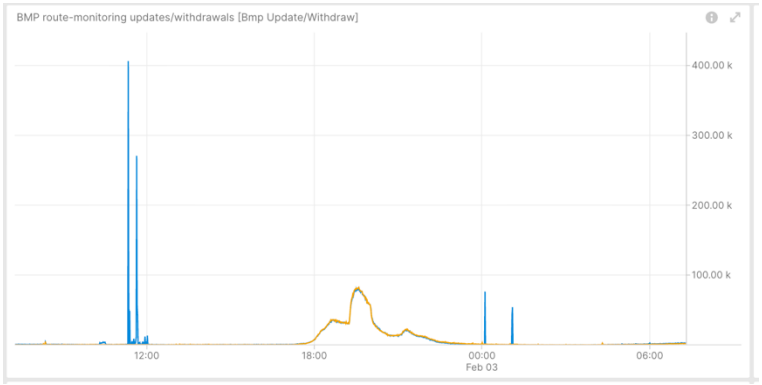
Leute Vermischtes

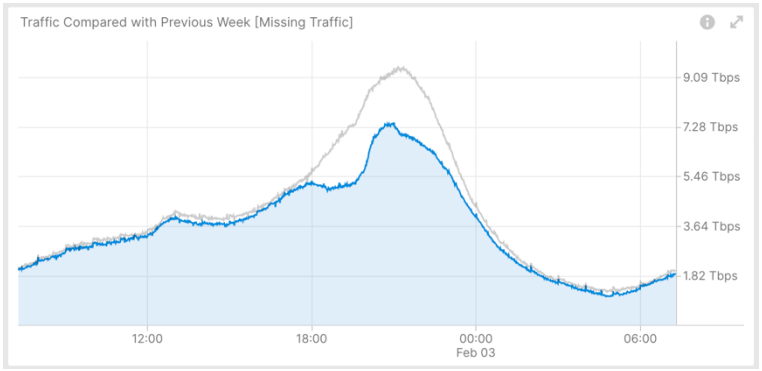
Startseite | Panorama | Störung bei Swisscom TV und Blue TV App behoben

Störung bei Swisscom

Swisscom-TV und blue TV App stehen wieder zur Verfügung

Nach teilweise stundenlangen Ausfällen bei Tausenden von Nutzern meldet das Telekomunternehmen um 22 Uhr, dass die Störungen behoben worden seien.



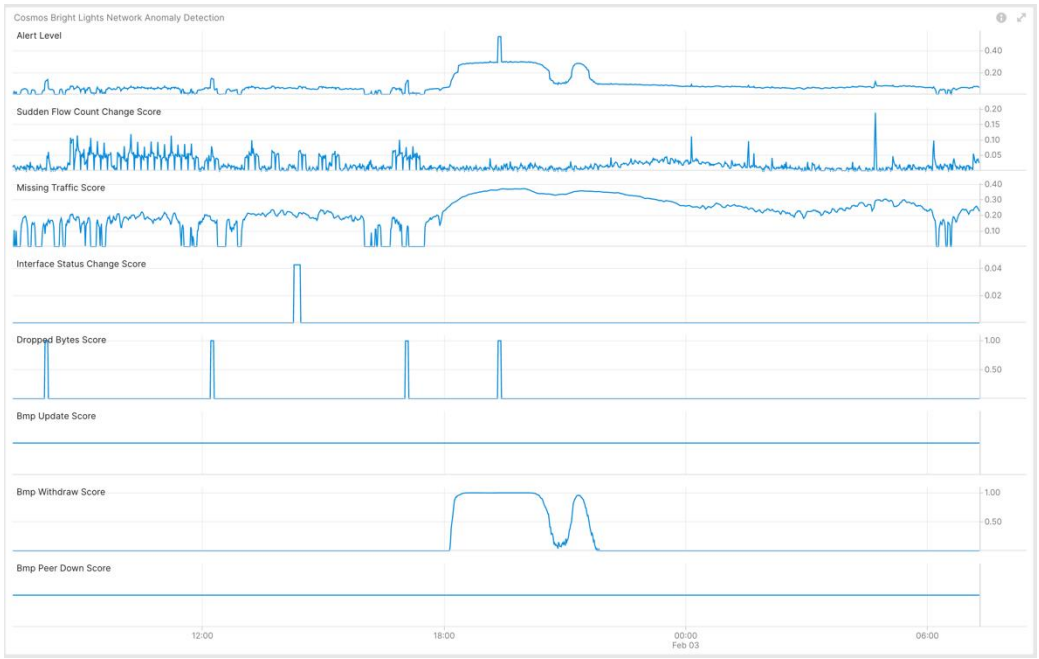


Network Anomaly Detection Architecture

Document implementation and operational experience

L3 VPN – Real-Time Incident Analysis

Concern Score: 0.53
Flow Count Spike: **0.03** Missing Traffic: **0.37** Traffic Drop: **1.00**
BMP Peer: **0.00** Interface Down: **0.00**
BMP Update: **0.00** BMP Withdrawal: **1.00**



- **BMP route-monitoring Update/Withdraw check detected continuous and excessive routing topology changes due to users restarting tv boxes.**
- BMP peer Down/Up check did not apply because the hardware crash happened at the application layer.
- Interface Down/Up check did not apply.
- **Traffic Drop spike recognized drops due to unstable routing topology.**
- **Missing Traffic** detected.
- Sudden increased or decreased Flow Count was not applicable.

Overall: data plane and control plane checks have detected the excessive routing topology changes with service disruption.

Semantic Metadata Annotation

DRAFT-IETF-NMOP-NETWORK-ANOMALY-SEMANTICS-05

Semantic Metadata Annotation

Document summary

Motivation:

Enable the exchange of network anomaly data across diverse systems and support benchmarking of anomaly detection solutions

Approach:

Define a standardized semantic metadata schema and a set of semantically structured terms

Outcome:

Provide human-readable context for describing and understanding network anomalies

Action	Reason	Trigger
Interface State	Up	Link-Layer
Interface State	Down	Link-Layer
Interface Statistics	Errors	-
Interface Statistics	Discards	-
Interface Statistics	Unknown Protocol	-

Table 3: Description of symptoms and their actions, reasons and triggers for Management Plane.

Semantic Metadata Annotation

Key draft updates since v-03

- **Terminology update**
  - Added missing definition of terminologies used in the draft such as concern score and symptom.
- **Schema change**
  - Removed unused typedef score
  - Refined vpn-node-termination
  - Introduced dedicated L2 & L3 groupings for service
- **Symptom table update**
  - Update symptom: reason “Previous” -> “Drop”, trigger “Time” -> “Outside Monitored Domain”
- Avro schema changed accordingly

```
augment /rsn:relevant-state/rsn:anomaly:
      +--rw vpn-node-terminations* [hostname vrf-name]
         +--rw hostname                inet:host
         +--rw vrf-id?                 uint32
         +--rw vrf-name                string
         +--rw route-distinguisher?    string
         +--rw interface-id*           uint32
         +--rw interface-name*         string
         +--rw peer-ip*                inet:ip-address
         +--rw next-hop*               inet:ip-address
```

```
augment /rsn:relevant-state-notification/rsn:service:
      +--:(l2vpn)
      |  +-- l2vpn-service* [vpn-id]
      |     +-- vpn-id                string
      |     +-- uri?                  inet:uri
      |     +-- vpn-name?             string
      |     +-- site-ids*             string
      |     +-- change-id?            yang:uuid
      |     +-- change-start-time?    yang:date-and-time
      |     +-- change-end-time?      yang:date-and-time
      +--:(l3vpn)
         +-- l3vpn-service* [vpn-id]
            +-- vpn-id                string
            +-- uri?                  inet:uri
            +-- vpn-name?             string
            +-- site-ids*             string
            +-- change-id?            yang:uuid
            +-- change-start-time?    yang:date-and-time
            +-- change-end-time?      yang:date-and-time
```

Semantic Metadata Annotation

Document implementation and operational experience

Snippet of message example from Cosmos Bright Lights Implementation


```
"vpnNodeTerminations": [
    {
        "hostname": "pcb05ro1010bew",
        "vrfId": null,
         " vrfName": "null",
        "routeDistinguisher": {
        "string": "0:64499:100196518"
    },
    "peerIp": [
        "138.187.124.33",
        "138.187.124.35"
    ],
    "nextHop": [],
    "interfaceId": [],
    "interfaceName": []
  }
],
"stage": "detection",
"operationalData":
  {
     " topicName”: null,
     " subjectName”: null
  }
```

```
"service": {
     "L3VpnServiceContainer": {
        "l3VpnService": [
           {
              "vpnId": "64497:59121",
              "uri": {
                 "string": "https://thor-ui.thoruipp.corproot.net/cantata/lcs?dstCommunity=64497:59121"
              },
              "vpnName": {
                 "string": "64497:59121"
              },
              "siteIds": null,
              "changeId": null,
              "changeStartTime": null,
              "changeEndTime": null
           }
        ]
     }
  }
```

Network Anomaly Lifecycle

DRAFT-IETF-NMOP-NETWORK-ANOMALY-LIFECYCLE-05

Network Anomaly Lifecycle

Document summary

Motivation:

Bridge the gap between automated network anomaly detection and actionable operational tasks

Approach:

Define a standardized, iterative lifecycle for Network anomaly

Outcome:

Continuously Improve the correctness of anomaly detection through human-in-the-loop feedback

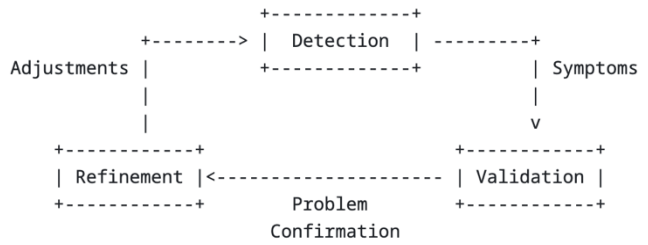


Figure 1: Anomaly Detection Refinement Lifecycle

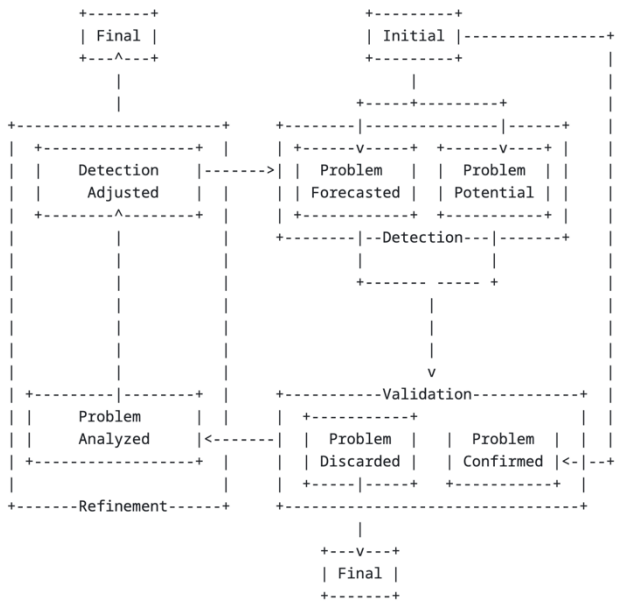


Figure 2: Network Anomaly State Machine

Network Anomaly Lifecycle

Key draft updates since v-03

- **Terminology update**
  - Renamed “state/phase” to “stage” to avoid confusion with protocol “states”.
- **Schema change**
  - Changed “state” -> “stage”
  - Fixed RFC 8407 related Yang warnings (remove mandatory false)
  - Include operational data in anomaly and introduce “message-broker-grouping”
- **Refinement**
  - Refined definition of confidence score and concern score
  - Optimized Figure 2
  - Consolidated the usage of score across different drafts

```
 leaf stage {
          type identityref {
            base network-anomaly-stage;
          }
          mandatory true;
          description
            "Stage of the relevant state.";
        }
```

```
grouping message-broker-grouping {
        description
          "References message broker draft-ietf-nmop-yang-
message-broker-integration entities.";
        leaf topic-name {
          type inet:host-name;
          description
            "From which message broker topic the
operational data was consumed from.";
        }
        leaf subject-name {
          type inet:host-name;
          description
            "To which message broker subject the
operational data references to.";
        }
      }
```

Next Steps and Remaining Issues

Feedback on latest changes

Next Steps

- Request YANG doctors review for draft-ietf-nmop-network-anomaly-semantics-05 and draft-ietf-nmop-network-anomaly-lifecycle-05.
- Implement semantic metadata in Cosmos Bright Lights to replace placeholder values for newly introduced fields, including
  - site-ids
  - interface names
  - VRF names
- Extend the postmortem system requirements, accompanied by an implementation PoC

Remaining Issues

- No known remaining issues at this time.