

An Architecture for a **Network Anomaly Detection** Framework

draft-ietf-nmop-network-anomaly-architecture-05

draft-ietf-nmop-network-anomaly-semantics-03

draft-ietf-nmop-network-anomaly-lifecycle-03

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

17. July 2025

Problem Statement and Motivation

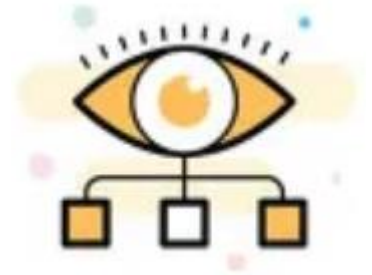
How it is being addressed in which document

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.

Network Anomaly Detection



- [draft-ietf-nmop-network-anomaly-architecture](#) describes the motivation and architecture and the relationship to other two documents.
- [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 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.

Network Anomaly Detection Architecture

Document Updates

- Updated terminology. Change from "cause" to "trigger" based on Adrian's feedback.
- Updated Service Disruption Detection Section to cover templates.
- Changed Service Model reference from [RFC 8309](#) to [RFC 8969](#).
- Merged editorial input from Rüdiger Geib (offlist), Reshad Rahman and Paul Aitken.
Thanks a lot for the review!

Semantic Metadata Annotation

Document Updates

- Updated YANG modules.
 - Added "template", see [section 3.2 in Network Anomaly Detection Architecture](#), and "season" into ietf-network-anomaly-symptom-cbl.
 - Added maintenance related information into ietf-network-anomaly-service-topology.
- Updated terminology. Change from "cause" to "trigger" based on Adrian's feedback.
- Added in Section 4.4 Apache AVRO data model translation.
- Completed Security Considerations according to [draft-ietf-netmod-rfc8407bis-28#appendix-B](#).
- Described service model context and added normative reference to RFC 8969.
- Added Cosmos Bright Lights in Implementation status section.

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

```
augment /rsn:relevant-state/rsn:anomaly/rsn:symptom:  
  +--rw action?      string  
  +--rw reason?      string  
  +--rw trigger?     string  
  +--rw network-plane? enumeration  
  +--rw template?    string  
  +--rw season?      Enumeration
```

```
module: ietf-network-anomaly-service-topology
```

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

Network Anomaly Lifecycle

Document Updates

- Updated relevant-state YANG module
 - Added global uri, confidence-score and strategy
 - Added service container
 - Renamed anomaly grouping from anomalies to anomaly according to [RFC 8407](#).
 - Annotator-type is now an enumeration.
- Merged terminology input from Adrian
- Completed Security Considerations according to [draft-ietf-netmod-rfc8407bis-28#appendix-B](#).
- Received review from Paul Aitken which will be addressed in -04.

```
module: ietf-relevant-state
  +--rw relevant-state
    +--rw id yang:uuid
    +--rw uri? inet:uri
    +--rw description? string
    +--rw start-time yang:date-and-time
    +--rw end-time? yang:date-and-time
    +--rw strategy? string
    +--rw confidence-score? score
    +--rw concern-score score
    +--rw (service)?
    +--rw anomaly* [id revision]
      +--rw id yang:uuid
      +--rw revision yang:counter32
      +--rw uri? inet:uri
      +--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? identityref
      +--rw annotator
        | +--rw id? yang:uuid
        | +--rw name string
        | +--rw version? string
        | +--rw annotator-type? enumeration
      +--rw symptom!
        +--rw id yang:uuid
        +--rw concern-score score
```

Network Anomaly Lifecycle and Semantic Metadata Annotation

Combined YANG Schema Tree

```

notifications:
  +---n relevant-state-notification
    +--ro publisher
      | +--ro id?          yang:uuid
      | +--ro name        string
      | +--ro version?    string
    +--ro id              yang:uuid
    +--ro uri?            inet:uri
    +--ro description?    string
    +--ro start-time      yang:date-and-time
    +--ro end-time?       yang:date-and-time
    +--ro smcblsymptom:strategy? string
    +--ro confidence-score? score
    +--ro concern-score   score
    +--ro (service)?
      | +--:(smtopology:l2vpn)
      | | +--ro smtology:vpn-service* [vpn-id]
      | | | +--ro smtology:vpn-id      string
      | | | +--ro smtology:uri?        inet:uri
      | | | +--ro smtology:vpn-name?    string
      | | | +--ro smtology:site-ids*    string
      | | | +--ro smtology:change-id?   yang:uuid
      | | | +--ro smtology:change-start-time? yang:date-and-time
      | | | +--ro smtology:change-end-time? yang:date-and-time
      | +--:(smtopology:l3vpn)
      | | +--ro smtology:vpn-service* [vpn-id]
      | | | +--ro smtology:vpn-id      string
      | | | +--ro smtology:uri?        inet:uri
      | | | +--ro smtology:vpn-name?    string
      | | | +--ro smtology:site-ids*    string
      | | | +--ro smtology:change-id?   yang:uuid
      | | | +--ro smtology:change-start-time? yang:date-and-time
      | | | +--ro smtology:change-end-time? yang:date-and-time

```

```

notifications:
  +---n relevant-state-notification
    +--ro anomaly* [id revision]
      +--ro id          yang:uuid
      +--ro revision    yang:counter32
      +--ro uri?        inet:uri
      +--ro state        identityref
      +--ro description? string
      +--ro start-time
        | yang:date-and-time
      +--ro end-time?
        | yang:date-and-time
      +--ro confidence-score? score
      +--ro pattern?        identityref
      +--ro annotator
        | +--ro id?          yang:uuid
        | +--ro name        string
        | +--ro version?    string
        | +--ro annotator-type? enumeration
      +--ro symptom!
        | +--ro id          yang:uuid
        | +--ro concern-score score
        | +--ro smcblsymptom:action? string
        | +--ro smcblsymptom:reason? string
        | +--ro smcblsymptom:trigger? string
        | +--ro smcblsymptom:network-plane? enumeration
        | +--ro smcblsymptom:template? string
        | +--ro smcblsymptom:season? Enumeration
      +--ro smtology:vpn-node-terminations*
        [hostname route-distinguisher]
        +--ro smtology:hostname      inet:host
        +--ro smtology:route-distinguisher string
        +--ro smtology:peer-ip*      inet:ip-address
        +--ro smtology:next-hop*      inet:ip-address
        +--ro smtology:interface-id* uint32

```

Shows
the observed
symptoms,
the network
dimensions
triggering and
connectivity
service impacted.

Network Anomaly Lifecycle and Semantic Metadata Annotation

Example Message from Cosmos Bright Lights Implementation

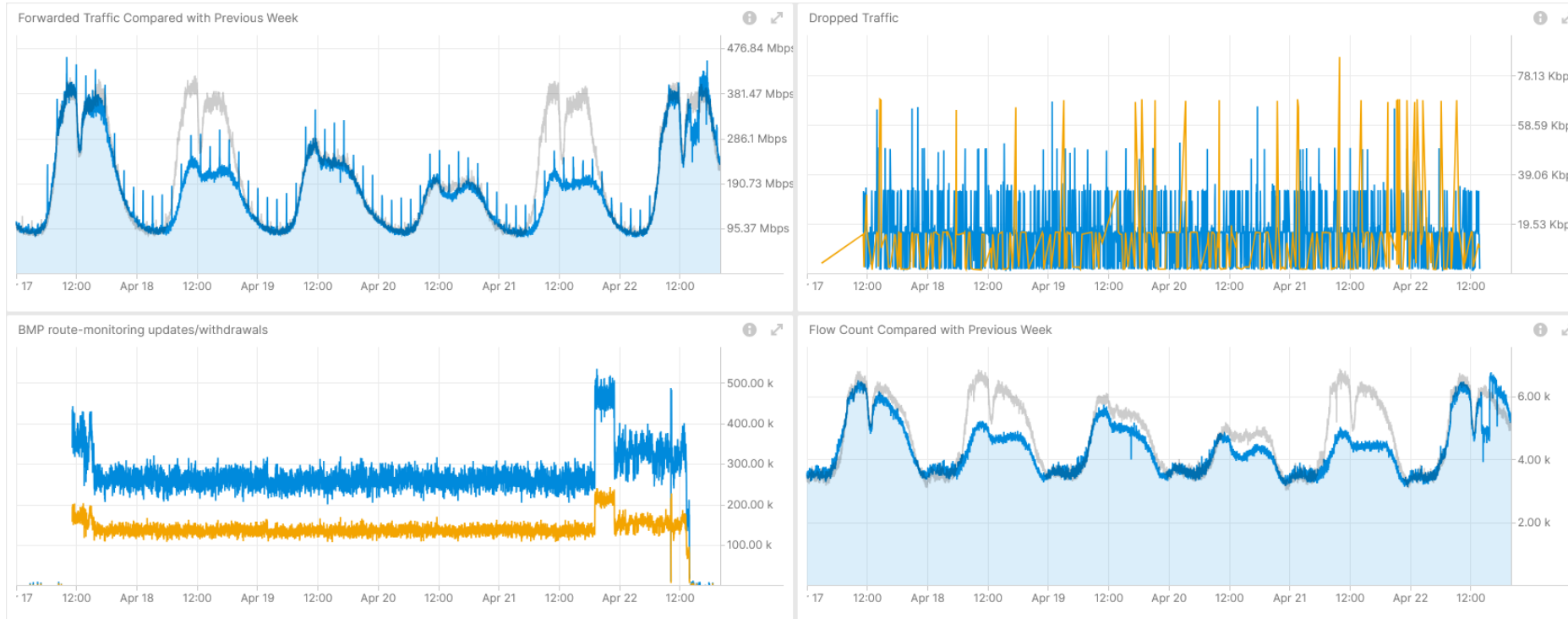
```
{
  "id": "616963b4-1f4f-4abe-94b5-7e1354653d49",
  "uri": {
    "string": "https://pivot-url-
proxy.app.zhh.sbd.corproot.net/pivot/c/926d/CBL_LC_Overview_Dev?vpn_id=64497:19313&co
mms=64497:19313"
  },
  "description": null,
  "startTime": 1745333220000,
  "endTime": {
    "long": 1745333280000
  },
  "confidenceScore": null,
  "concernScore": 8,
  "anomaly": [
    {
      "id": "ffdfb6d8-2a00-5219-b458-add2ce57e2db",
      "revision": 0,
      "uri": null,
      "state": "detection",
      "description": null,
      "startTime": 1745332860000,
      "endTime": {
        "long": 1745333220000
      },
      "confidenceScore": null,
      "pattern": null,
      "annotator": {
        "id": {
          "string": "ffdfb6d8-2a00-5219-b458-add2ce57e2db"
        },
        "name":
"com.swisscom.daisy.cosmos.brightlights.bmp.functions.BmpCountScoringPerWindow",
        "annotatorType": {
          "AnnotatorType": "algorithm"
        }
      },
      "symptom": {
        "Symptom": {
          "id": "1bee6d7e-923b-4990-b33f-208ed1bd9cf4",
          "concernScore": 0,
          "action": null,
          "reason": null,
          "trigger": null,
          "networkPlane": null
        }
      }
    }
  ]
}
```

```
"vpnNodeTerminations": [
  {
    "hostname": "138.190.128.227",
    "routeDistinguisher": "2:4260047718:10440",
    "peerIp": [
      "10.94.87.138"
    ],
    "nextHop": [],
    "interfaceId": []
  },
  {
    "service": {
      "L3VpnServiceContainer": {
        "L3VpnService": [
          {
            "vpnId": "64497:19313",
            "uri": {
              "string": "https://thor-
ui.thoruipp.corproot.net/cantata/lcs?dstCommunity=64497:19313"
            },
            "vpnName": {
              "string": "64497:19313"
            },
            "siteIds": null,
            "changeId": null,
            "changeStartTime": null,
            "changeEndTime": null
          }
        ]
      }
    },
    "publisher": {
      "id": "161495ba-3c0a-5f13-90ae-b907259be226",
      "name": "Brightlights - Streaming",
      "version": {
        "string": "1.0.9-alert-1"
      }
    }
  }
]
```

Shows
the observed
symptoms,
the network
dimensions
triggering and
connectivity
service impacted.

April 17-22th, OSPF/BGP Routing Instability

64497:471 L3 VPN – Real-Time Incident Analysis



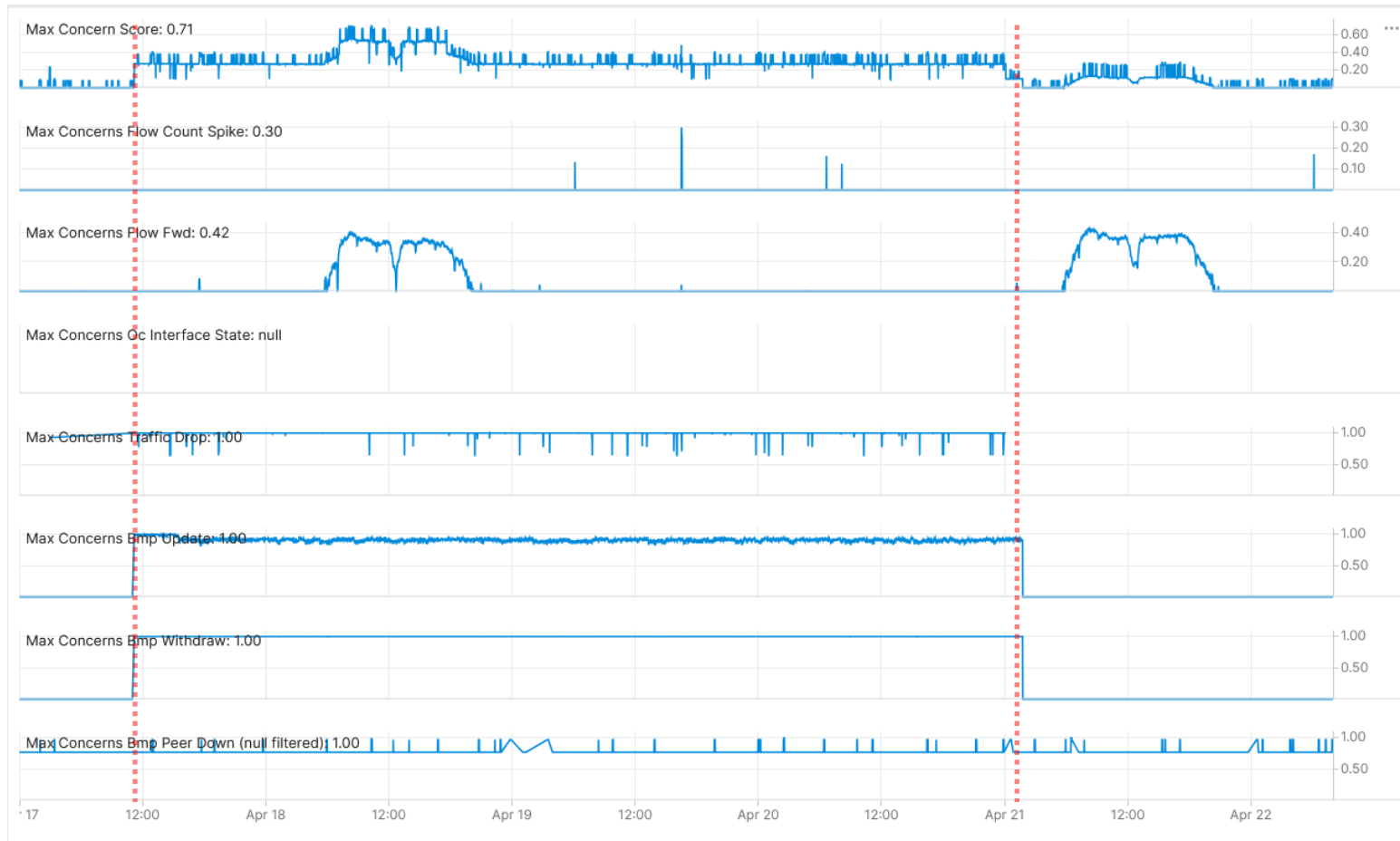
Shows traffic bad TTL, adjacency drops and traffic volume changes due to public holidays, Measured with IPFIX and Correlated with BGP VPNv4/6.

Shows constant BGP topology changes and flow count changes due to public holidays. Measured with IPFIX and Correlated with BGP VPNv4/6, BMP Adj-RIB In and Local RIB.

Operational Network Telemetry forwarding plane, IPFIX, BMP measured control plane metrics.

April 17-22th, OSPF/BGP Routing Instability

64497:471 L3 VPN – Network Anomaly Detection – Live



Cosmos Bright Lights monitoring 64497:471 L3 VPN in real-time during maintenance window.

Concern Score: **0.71**
Flow Count Spike: **0.30**
Missing Traffic: **0.41**
Traffic Drop: **1.00**
BMP Peer: **0.96**
Interface Down: **0.00**
BMP Update: **1.00**
BMP Withdrawal: **1.00**



BMP route-monitoring
Update/Withdraw check recognized **excessive topology changes.**



BMP peer Down/Up check recognized issue with **unstable peer on another network platform..**



Interface Down/Up check did not apply.



Traffic Drop spike recognized drops due to instable routing topology.



Missing Traffic recognized traffic volume changes **due to public holidays.**



Increased or decreased Flow Count was not applicable.



Overall: 2 out of 6 checks have detected the excessive routing topology changes with drops. Customer profiling related false positives see in conclusion.

April 17-22th, OSPF/BGP Routing Instability

Provider Impact Analysis – Concern Objects declare Causality

Concerning Bmp Router list		detected BGP peer down	
Bmp Router	Count ↓	Time, detected peer down	Count
138.190.128.227	3,337	Apr 17, 19:36-19:37	1
138.190.128.226	48	peer_ip=10.94.87.130, bmp_router=138.190.128.227, rd=2:4260047718:10442	1
138.190.128.225	24	Apr 17, 19:37-19:38	1
		peer_ip=10.94.87.130, bmp_router=138.190.128.227, rd=2:4260047718:10442	1
		Apr 17, 19:38-19:39	3
		peer_ip=10.94.87.130, bmp_router=138.190.128.227, rd=2:4260047718:10442	3
		Apr 17, 19:39-19:40	1
		peer_ip=10.94.87.130, bmp_router=138.190.128.227, rd=2:4260047718:10442	1
		Apr 17, 19:40-19:41	1

Concerning node with interface status change		Detected interface up	Detected interface down
Node Id	Count ↓	Time, detected interface up	Count
			Time, detected interface down
			Count

Showing excessive BGP peer downs on MPLS Inter-AS Option A Platform unrelated to Incident.
Measured with BMP Adj-RIB In.

Analytical Cosmos Bright Lights observed metrics.

April 17-22th, OSPF/BGP Routing Instability

Semantic Metadata Annotation - National Holidays



**Operational Network Telemetry forwarding plane,
IPFIX, BMP measured control plane metrics.**

```
+++ro symptom!  
|   +-ro id                               yang:uuid  
|   +-ro concern-score                   score  
|   +-ro smcblsymptom:action?            string  
|   +-ro smcblsymptom:reason?            string  
|   +-ro smcblsymptom:trigger?           string  
|   +-ro smcblsymptom:network-plane?     enumeration  
|   +-ro smcblsymptom:strategy?          string  
|   +-ro smcblsymptom:template?         string  
|   +-ro smcblsymptom:season?            Enumeration
```

**National holiday
information
should be
considered to
improve accuracy
of Contextual
outliers for
seasonal traffic
volume and flow
count change
categorized
profiles in the
missing traffic and
flow count spike
strategies and
declared in
symptom
semantics.**

Next Steps and Remaining Issues

Feedback on latest changes, YANG Doctors review, SIMAP Integration

Next Steps

- Requesting working group feedback on the updated YANG models and editorial changes.
- Request YANG doctors review for [draft-ietf-nmop-network-anomaly-semantics-03](#) and [draft-ietf-nmop-network-anomaly-lifecycle-03](#).

Remaining Issue

- Clarify with working group relationship between rule-based and knowledge-based.
- smtology:vpn-node-terminations defines hostname, route-distinguisher, peer-ip and next-hop and interface-id instead of augmenting /nw:networks/nw:network/nw:node:termination-point from [Section 4.2 of RFC 8345](#).
- How should we address to achieve Postmortem Replay in SIMAP, [Section 3.9 of draft-ietf-nmop-simap-concept](#).