

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

16. July 2025

Problem Statement and Motivation

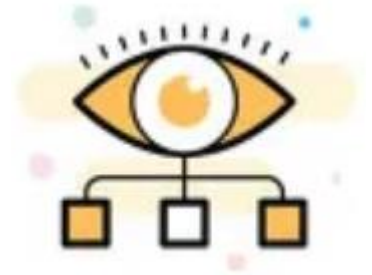
How it is being addressed in which document

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, Reshad and Paul. 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](https://datatracker.ietf.org/drafts/netmod/rfc8407bis-28#appendix-B).

```
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

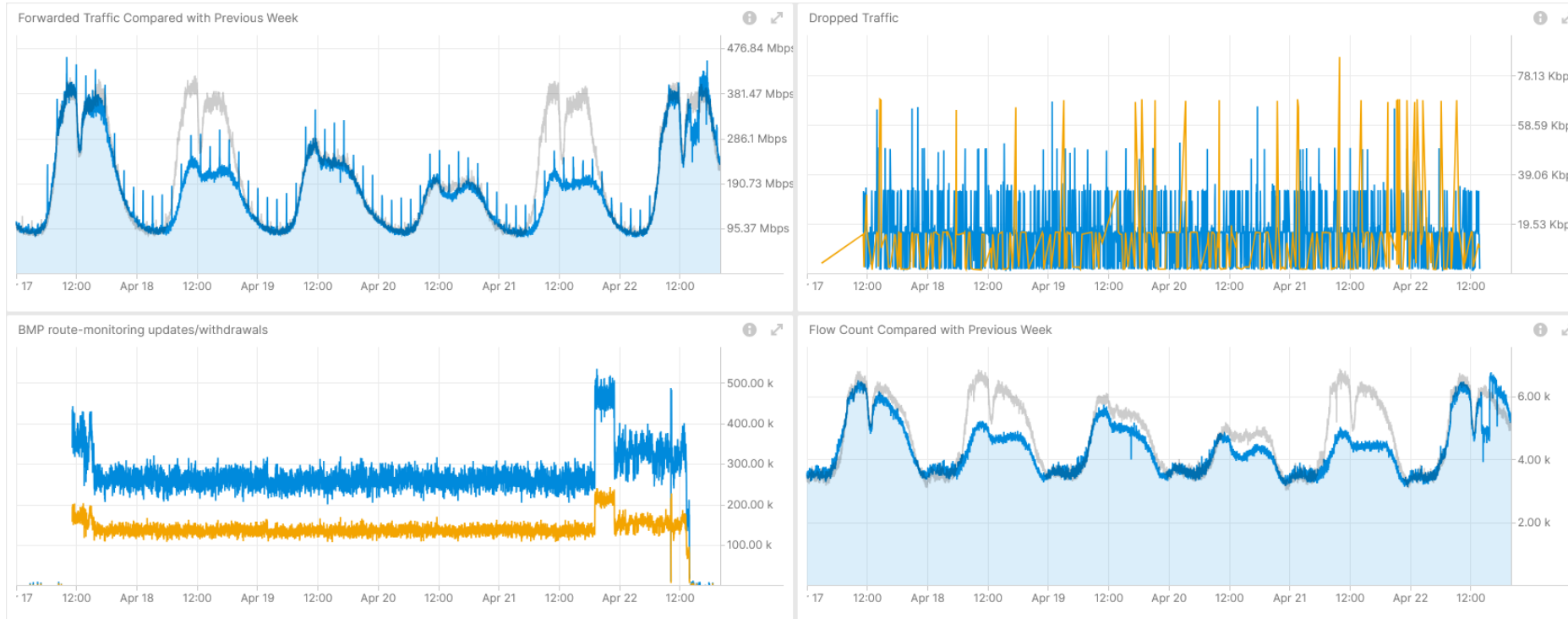
```
{
  "id": "616963b4-1f4f-4abe-94b5-7e1354653d49",
  "uri": {
    "string": "https://pivot-url-
proxy.app.zhh.sbd.corproot.net/pivot/c/926d/CBL_LC_Overview_Dev?vpn_id=64497:19313&co
mms=64497:19313"
  },
  "description": null,
  "startTime": 1745333220000,
  "endTime": {
    "long": 1745333280000
  },
  "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



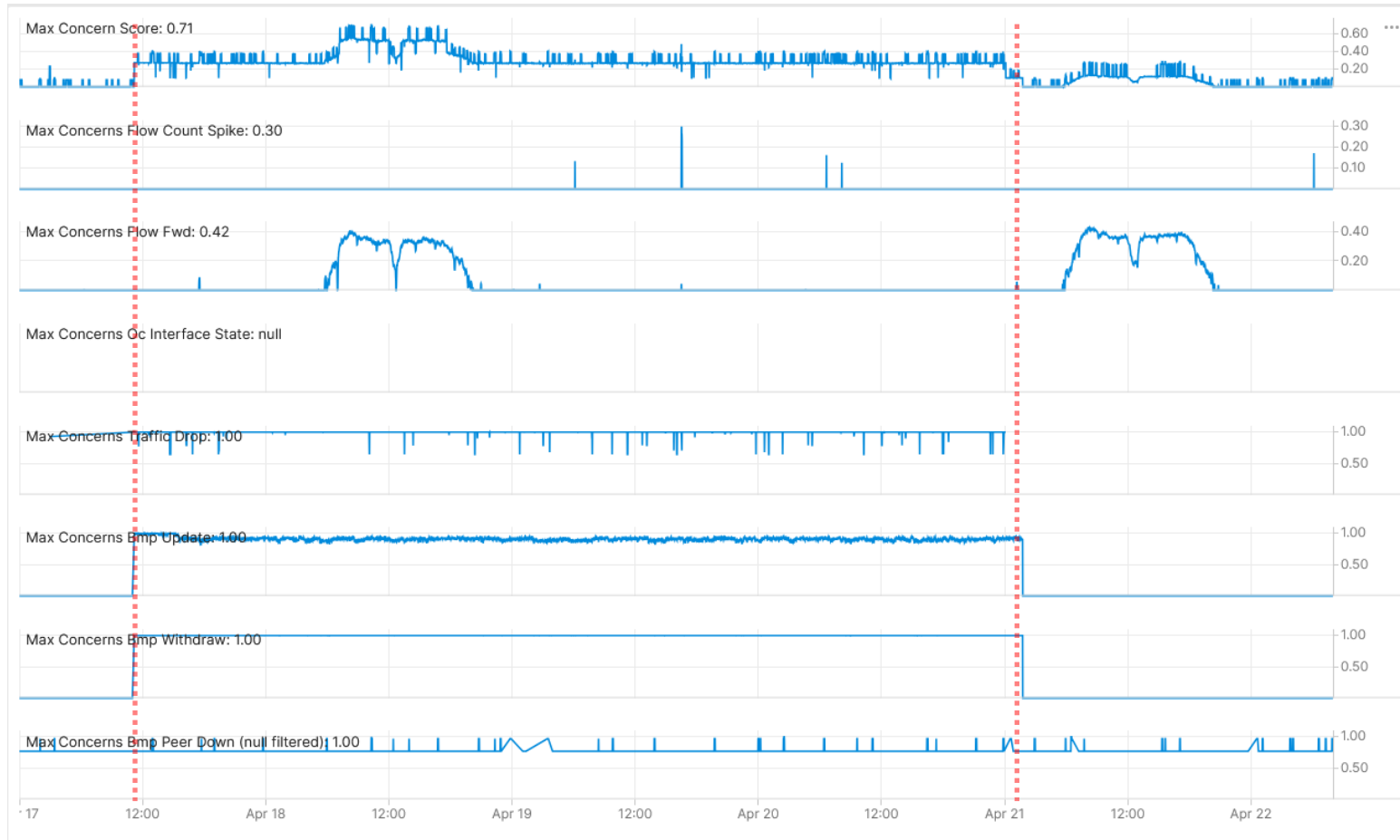
Shows **traffic bad TTL**, **adjacency drops** and **traffic volume changes** due to public holidays, Measured with IPFIX and Correlated with BGP VPNv4/6.

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/Interface Down: **0.96/0.00**

BMP Update/Withdrawal: **1.00/1.00**



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 triggered sporadically **due to public holidays** flow count changes.



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

Provider Impact Analysis – Concern Objects declare Causality

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

10

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](#).

Relevant Papers for more Details

Practical Anomaly Detection in Internet Services: An ISP centric approach

Alex Huang Feng*, Pierre Francois*, Kensuke Fukuda¹, Wanting Du¹,
Thomas Graf¹, Paolo Lucente¹, Stéphane Frénot*

*INSA Lyon, Inria, CITI, UR3720, Villeurbanne, France
alex.huang-feng@insa-lyon.fr, pierre.francois@insa-lyon.fr, stephane.frenot@insa-lyon.fr
¹National Institute of Informatics, Tokyo, Japan
kensuke@nii.ac.jp
¹Swisscom, Zurich, Switzerland
wanting.du@swisscom.com, thomas.graf@swisscom.com
¹pmacct.net, Barcelona, Spain
paolo@pmacct.net

Abstract—Identifying anomalies in a network is a crucial endeavor for Internet Service Providers (ISPs). Anomalies that impact the traffic of the ISP customers can lead to a degradation in the reputation of the company. Moreover, silent anomalies that do not break connectivity can impact the revenue and business of ISPs. Therefore, monitoring and anomaly detection has become essential for ISPs. In this paper, we present an ongoing research project aimed at identifying anomalies in Internet services provided by an ISP. We aim at detecting anomalies within the domain managed by the ISP that impact the customer and the business of the ISP. We propose a rule-based approach designed to promptly detect and provide reporting for such anomalies in near real time, giving information that allows the operator to identify whether a solution can be brought. In this paper, we describe the collected network telemetry metrics and illustrate how they are processed using open-source solutions. We introduce a set of use cases showing that an ISP can monitor Internet services using IETF standard metrics.

1. INTRODUCTION

Internet services include providing global Internet reachability for customer Autonomous Systems (ASes) connected to an Internet Service Provider (ISP) and serving private customers within the ISP (e.g. FTTH). Disruptions in the network that affect the connectivity of an ISP not only significantly degrade the organization's reputation but also have implications on the company's revenue. Customers subscribed to Internet services depend on the ISP peering to reach the Internet and an incident between them and the Internet can have detrimental implications for their business.

Today, routing between different ASes is established using BGP [1]. ISPs managing an AS configure policies in their routers based on the business relationship they have with their neighboring ASes. Generally, ISPs classify their BGP neighbors into Customers, Settlement-free Peers and Transit Providers. Customer ASes compensate the ISP to reach the Internet. Settlement-free peers are mutual arrangements between two ISPs to exchange Internet traffic without any financial compensation and Transit Providers provide access to the global Internet.

ISPs rely on collected BGP messages and traffic counters to monitor peering and detect anomalies that could impact their customers. They closely supervise network traffic to identify unexpected patterns or potential abuses by peers. This underscores the importance for ISPs to receive prompt alerts when anomalous or unwanted traffic behaviors occur, enabling network operators to rapidly implement solutions and address the detected issues.

Anomaly detection (AD) has been a hot topic in the last decade where researchers have proposed new ways to detect irregularities in the data. Most research projects aiming at detecting anomalies in BGP networks use public repositories such as Routeviews and RIPE NCC archives [2, 3], allowing researchers to identify problems in Internet from a global point of view. In conjunction with publicly known incidents, researchers have been able to develop methods to detect anomalies in data from the public domain, with a focus on detecting anomalies in the global Internet topology [4, 5]. Simulated environments mimicking the deployed network and manually generated anomalies have also been used to test anomaly detection [6]. Very few projects use production data coming from an ISP to detect anomalies and root cause analysis within a single domain. AD within an AS have only been investigated by very few researchers having access to production data [7]–[9].

In this paper, we focus on detecting anomalies within a single AS to potentially help them fixing their configuration and find unwanted traffic flows impacting their business. We describe the target use cases in Section II. Instead of solely using BGP activity as a source of data, as done in [7], we use a larger set of monitoring information, allowing us to cover a broader set of service anomalies (Sec. III-A). The authors in [8] focus on detecting performance issues from end-to-end users, while the work presented in this paper also covers anomalies impacting the traffic from peering. In [9], anomaly detection is based on traffic information with a focus on network intrusion detection, while the project presented

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

Thomas Graf
thomas.graf@swisscom.com
Swisscom
Zurich, Switzerland

Pierre Francois
pierre.francois@insa-lyon.fr
Univ Lyon, INSA Lyon, Inria,
CITI, EA3720
Villeurbanne, France

Wanting Du
wanting.du@swisscom.com
Swisscom
Zurich, Switzerland

Stéphane Frenot
stephane.frenot@insa-lyon.fr
Univ Lyon, INSA Lyon, Inria,
CITI, EA3720
Villeurbanne, France

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>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ANRW '23, July 24, 2023, San Francisco, CA, USA
© 2023 Copyright held by the owner(s). Publication rights licensed to ACM.
ACM ISBN 979-4-4007-0274-7/23\$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.

Paper “Practical Anomaly Detection in Internet Services: An ISP centric approach”

Published at AnNet Workshop (In conjunction with IEEE NOMS)
Seoul, South Korea (6–10 May 2024)

Open access: <https://hal.science/hal-04655324>

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>