

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

draft-netana-nmop-network-anomaly-architecture-00

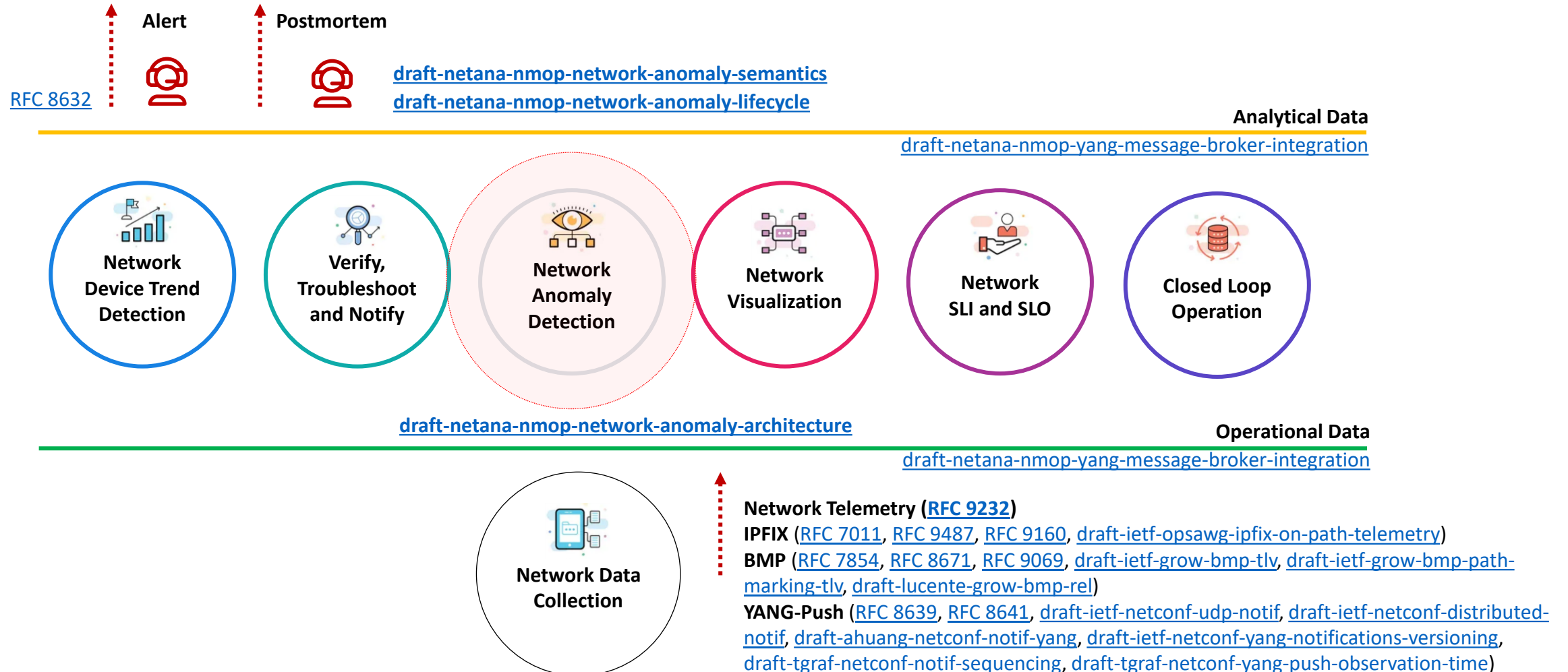
Motivation and architecture of a Network Anomaly Detection Framework
and the relationship to other documents describing
network symptom semantics and network incident lifecycle

wanting.du@swisscom.com
pierre.francois@insa-lyon.fr
thomas.graf@swisscom.com
vincenzo.riccobene@huawei-partners.com

14. July 2024

Data Mesh organizes Data in Organizations

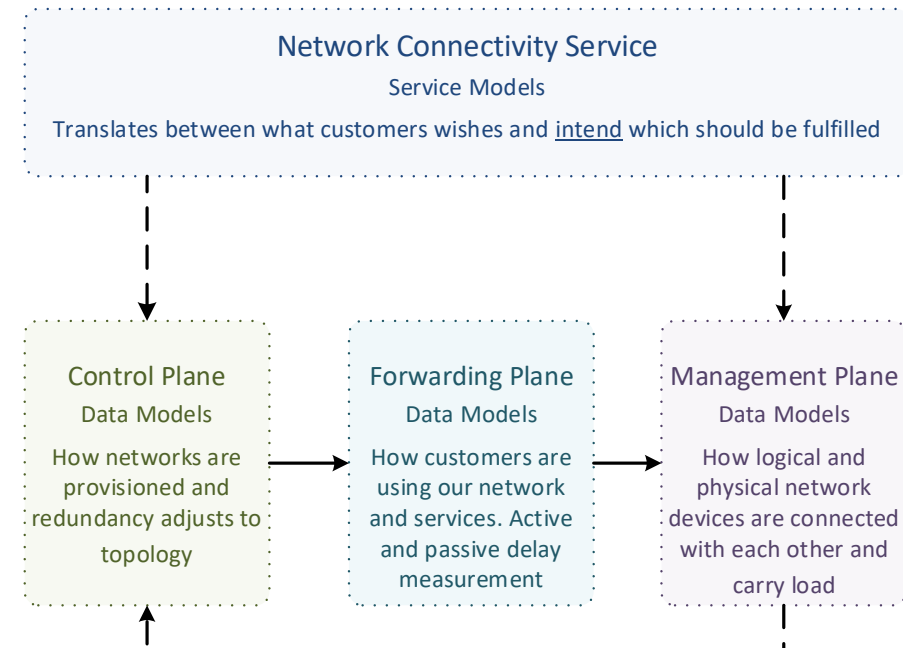
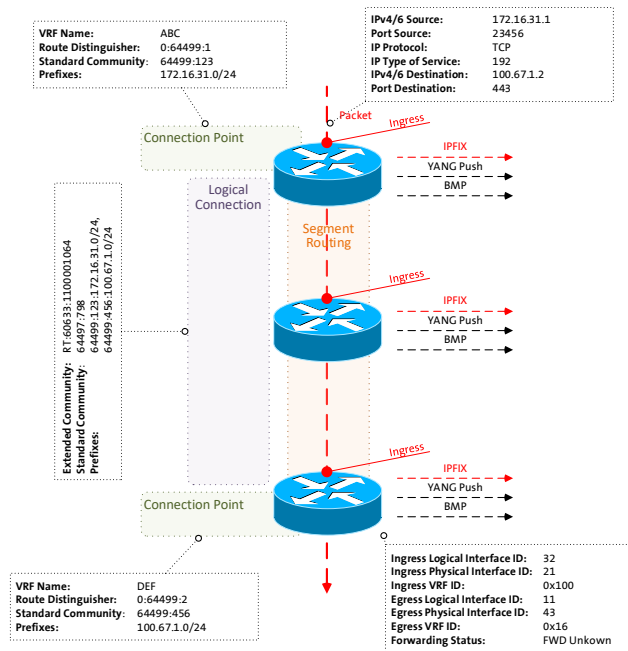
Enables Network Analytics use cases



Which operational metrics are collected

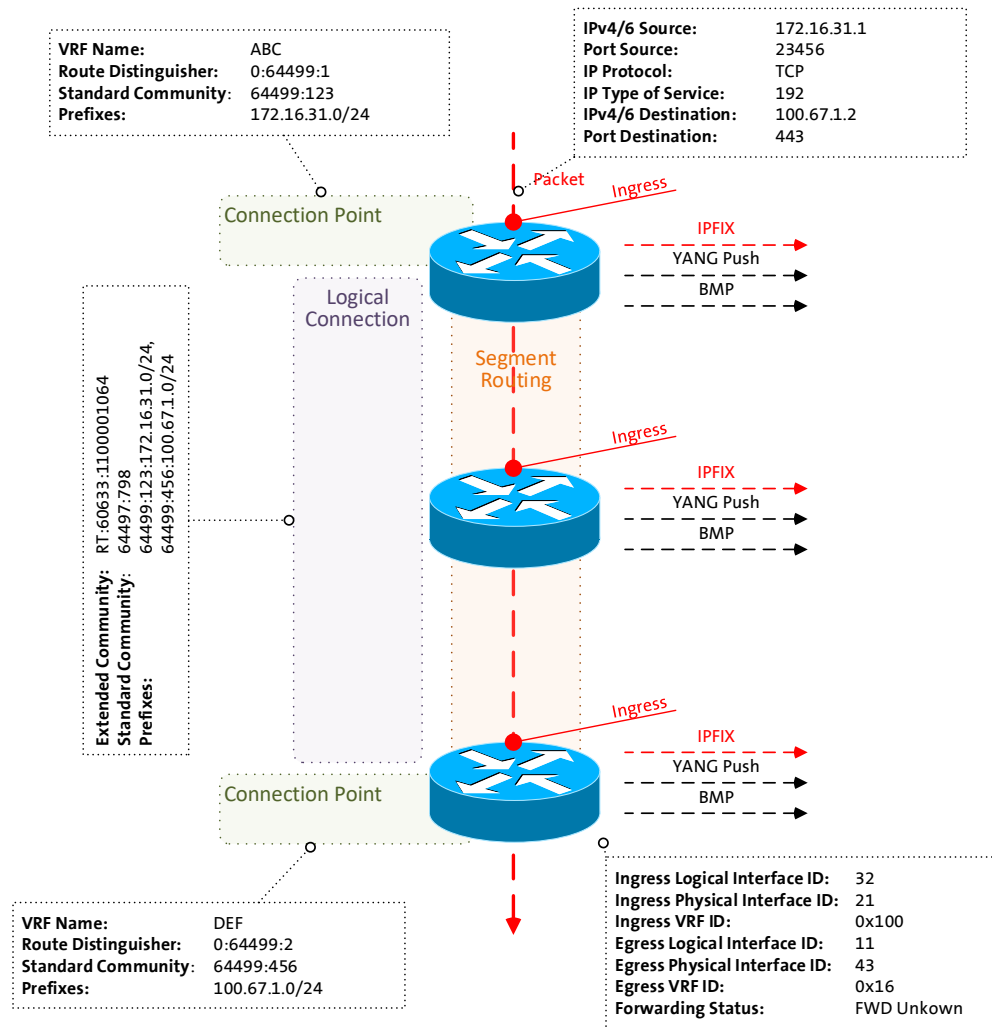
« Network operators **connect customers in** routing tables called **Connectivity Services** »

« Network Telemetry
(RFC 9232) describes how to collect data
from all 3 network planes efficiently »



Monitoring L3 VPN's with IPFIX, BMP and YANG Push

From Connectivity Service to Realtime Network Analytics



- > **Connectivity Service perspective**, Connection Points are connected through Logical Connections.
- > **From a BGP control-plane perspective**, IPv4/6 unicast prefixes in VRF's are tagged with BGP standard communities.
 - > One BGP standard community to identify the Logical Connection. One BGP standard community to identify each Connection Point.
 - > When IPv4/6 prefixes are exported from VRF's, a BGP route-distinguisher, BGP extended community route-targets and a SRv6 VPN SID for the IPv6 next-hop are allocated.
- > **From a forwarding plane perspective**, when IPv4/6 unicast traffic is received from the edge at the SRv6 PE, a lookup is performed, the SRv6 VPN SID is obtained and IPv6 next-hop is added when forwarded to the core.
- > **Swisscom collects** MPLS and SRv6 provider data plane, IPv4/6 unicast customer data-plane in IPFIX and at provider edge BGP VPNv4/6 unicast **in production** to perform real-time data correlation.

Segment Routing IPv6 Encapsulation

RFC 9487 provides IPFIX Visibility

> Provider data-plane

Divided into an IPv6 and Segment Routing Header.

The IPv6 header shows from which PE to which next-hop it is being forwarded. The Segment Routing Header the list of segments this packet needs to pass through and points to the active segment.

> Customer data-plane

This is what we receive from the customer and encapsulate for transport through the SRv6 core.

No.	Time	Source IP	Source Port	Destination IP	Destination Port	Protocol
7	2022-12-22 13:50:12.823123	203.0.113.46		203.0.113.30		ICMP
8	2022-12-22 13:50:12.823197	203.0.113.30		203.0.113.46		ICMP

>	Frame 7: 234 bytes on wire (1872 bits), 214 bytes captured (1712 bits)
>	Ethernet II, Src: HuaweiTe_3a:2e:62 (f8:53:29:3a:2e:62), Dst: HuaweiTe_3a:33:a2 (f8:53:29:3a:33:a2)
>	Internet Protocol Version 6, Src: 2001:db8:3::1, Dst: 2001:db8:18:0:10::
>	0110 = Version: 6
> 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
> 0000 00.. = Differentiated Services Codepoint: Default (0)
> 0000 0000 = Explicit Congestion Notification: Not ECN-Capable
> 0011 0001 1101 0001 1101 = Flow Label: 0x31d1d
>	Payload Length: 180
>	Next Header: Routing Header for IPv6 (43)
>	Hop Limit: 253
>	Source Address: 2001:db8:3::1
>	Destination Address: 2001:db8:18:0:10::
>	Routing Header for IPv6 (Segment Routing)
>	Next Header: IPIP (4)
>	Length: 11
>	[Length: 96 bytes]
>	Type: Segment Routing (4)
>	Segments Left: 1
>	Last Entry: 3
>	Flags: 0x00
>	Tag: 0000
>	Address[0]: 2001:db8:2:0:40::
>	Address[1]: 2001:db8:18:0:10::
>	Address[2]: 2001:db8:17:0:10::
>	Address[3]: 2001:db8:14:0:10::
>	Internet Protocol Version 4, Src: 203.0.113.46, Dst: 203.0.113.30
>	0100 = Version: 4
> 0101 = Header Length: 20 bytes (5)
>	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
>	Total Length: 84
>	Identification: 0x0bdf (3039)
>	010. = Flags: 0x2, Don't fragment
>	...0 0000 0000 0000 = Fragment Offset: 0
>	Time to Live: 63
>	Protocol: ICMP (1)
>	Header Checksum: 0xb77c [validation disabled]
>	[Header checksum status: Unverified]
>	Source Address: 203.0.113.46
>	Destination Address: 203.0.113.30
>	Internet Control Message Protocol

BMP – Address Family Agnostic

RFC 9069 provides Local RIB Visibility

> BMP Per Peer Header

Shows at **which RIB** (Adj-RIB In, Local or Adj-RIB Out, Pre or Post Policy) and from **which Peering** the BGP PDU at **which time** was obtained.

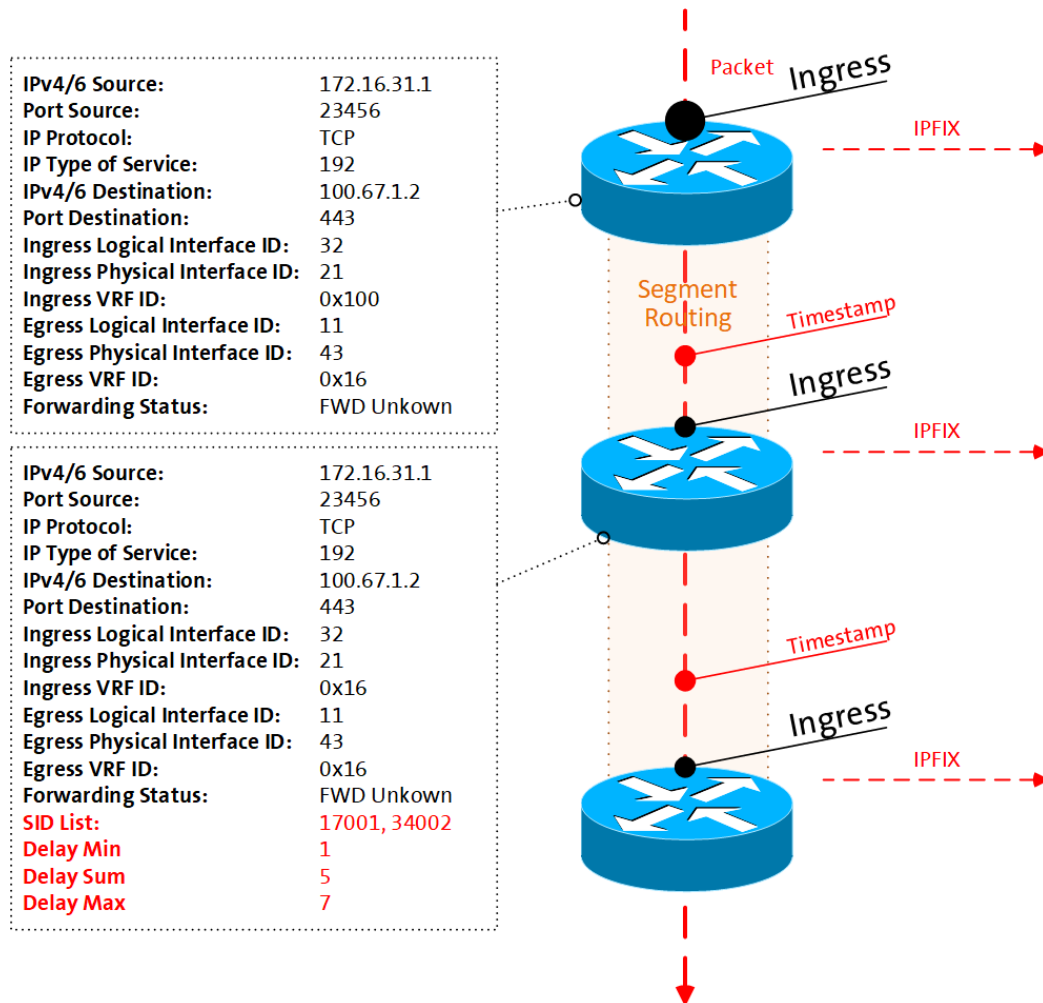
> Encapsulated BGP PDU

Shows the encapsulated BGP PDU. In case of BMP route-monitoring, it describes whether it was a topology **update or withdrawal** and for **BGP community, NLRI and BGP Prefix SID** path attributes.

No.	Time	Source IP	Destination IP	Protocol	Length	Info
10	2023-11-06 22:12:33.943442	2001:db8:2::1	2a02:a90:4007::4:2	BGP	1294	UPDATE Message
<						
> Frame 10: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits)						
> Ethernet II, Src: Cisco_ff:dd:90 (40:06:d5:ff:dd:90), Dst: VMware_0e:d8:14 (00:0c:29:0e:d8:14)						
> Internet Protocol Version 6, Src: 2001:db8:2::1, Dst: 2a02:a90:4007::4:2						
> Transmission Control Protocol, Src Port: 39041, Dst Port: 1792, Seq: 746, Ack: 1, Len: 1220						
✓ BGP Monitoring Protocol, Type Route Monitoring						
Version: 3						
Length: 227						
Type: Route Monitoring (0)						
✓ Per Peer Header						
Type: Loc-RIB Instance Peer (3)						
> 0000 0000 = Flags: 0x00						
Peer Distinguisher: 0:0						
Unused: 000000000000000000000000						
Address: 0.0.0.0						
ASN: 65536						
BGP ID: 198.51.100.191						
Timestamp (sec): 1699272753						
Timestamp (msec): 942134						
✓ Border Gateway Protocol - UPDATE Message						
Marker: ffffffffffffffffffffffffffffffff						
Length: 179						
Type: UPDATE Message (2)						
Withdrawn Routes Length: 0						
Total Path Attribute Length: 156						
✓ Path attributes						
> Path Attribute - MP_REACH_NLRI						
> Path Attribute - ORIGIN: IGP						
> Path Attribute - AS_PATH: empty						
> Path Attribute - MULTI_EXIT_DISC: 0						
> Path Attribute - LOCAL_PREF: 16400						
> Path Attribute - COMMUNITIES: 64496:299 64496:1001 64497:1 64499:1						
> Path Attribute - EXTENDED_COMMUNITIES						
✓ Path Attribute - BGP Prefix-SID						
> Flags: 0xc0, Optional, Transitive, Complete						
Type Code: BGP Prefix-SID (40)						
Length: 37						
✓ SRV6 L3 Service						
Type: SRV6 L3 Service (5)						
Length: 34						
Reserved: 00						
✓ SRV6 Service Sub-TLVs						
✓ SRV6 Service Sub-TLV - SRV6 SID Information						
Type: SRV6 SID Information (1)						
Length: 30						
Reserved: 00						
SRV6 SID Value: 2001:db8:1::						
SRV6 SID Flags: 0x00						
SRV6 Endpoint Behavior: End.DT4 with NEXT-CSID (0x003f)						
Reserved: 00						
✓ SRV6 Service Data Sub-Sub-TLVs						
✓ SRV6 Service Data Sub-Sub-TLV - SRV6 SID Structure						
Type: SRV6 SID Structure (1)						
Length: 6						
Locator Block Length: 32						
Locator Node Length: 16						
Function Length: 16						
Argument Length: 0						
Transposition Length: 16						
Transposition Offset: 48						

Measure On-Path Delay with Network Context

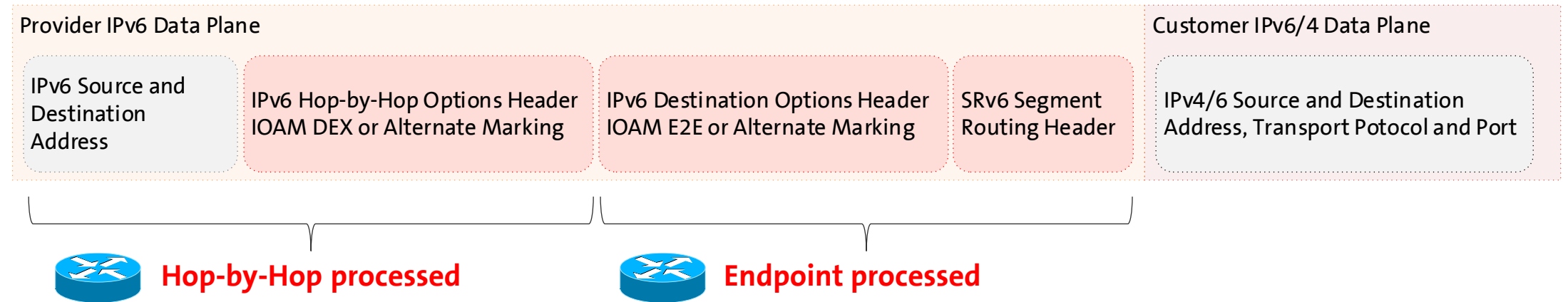
With draft-ietf-opsawg-ipfix-on-path-telemetry



- > Packets are **captured** ingress with an **optional sampler**, data plane dimensions **extracted, enriched** with management and control plane dimensions and added with a unique **flow ID** to a flow cache on the node for aggregation.
- > **A direct export marking bit and optionally a timestamp is added** to the packet when entering the OAM domain by leveraging Enhanced Alternate Marking ([RFC 9341](#), [draft-zhou-ippm-enhanced-alternate-marking](#)) or IOAM ([RFC 9378](#)) Direct Export or E2E Option Type.
- > Each subsequent packet for the same flow increases byte and packet count. Each new flow creates a new flow ID in the flow cache.
- > **At each node** in transit or only at the decapsulation node, **delay is calculated** by comparing the observation timestamp in the packet and when packet is received. **Delay is populated into the flow cache together with packet and byte count** as defined in [draft-ietf-opsawg-ipfix-on-path-telemetry](#).

IPFIX provides statistical data plane visibility

Comprehensive IPv6 data plane coverage



- > [draft-ietf-opsawg-ipfix-on-path-telemetry](#) defines OAM agnostic on-path delay IPFIX entities.
- > [draft-ietf-opsawg-ipfix-alt-mark](#) defines Alternate Marking IPFIX entities.
- > [draft-spiegel-ippm-ioam-rawexport](#) defines IOAM IPFIX entities.
- > [RFC 9487](#) defines Segment Routing Header IPFIX entities



Network Observability

System Demo

Detect L3 VPN Topology changes
and its Forwarding Plane impact
in **Near Real-Time**

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.

What our motivation is

Automate learn and improve

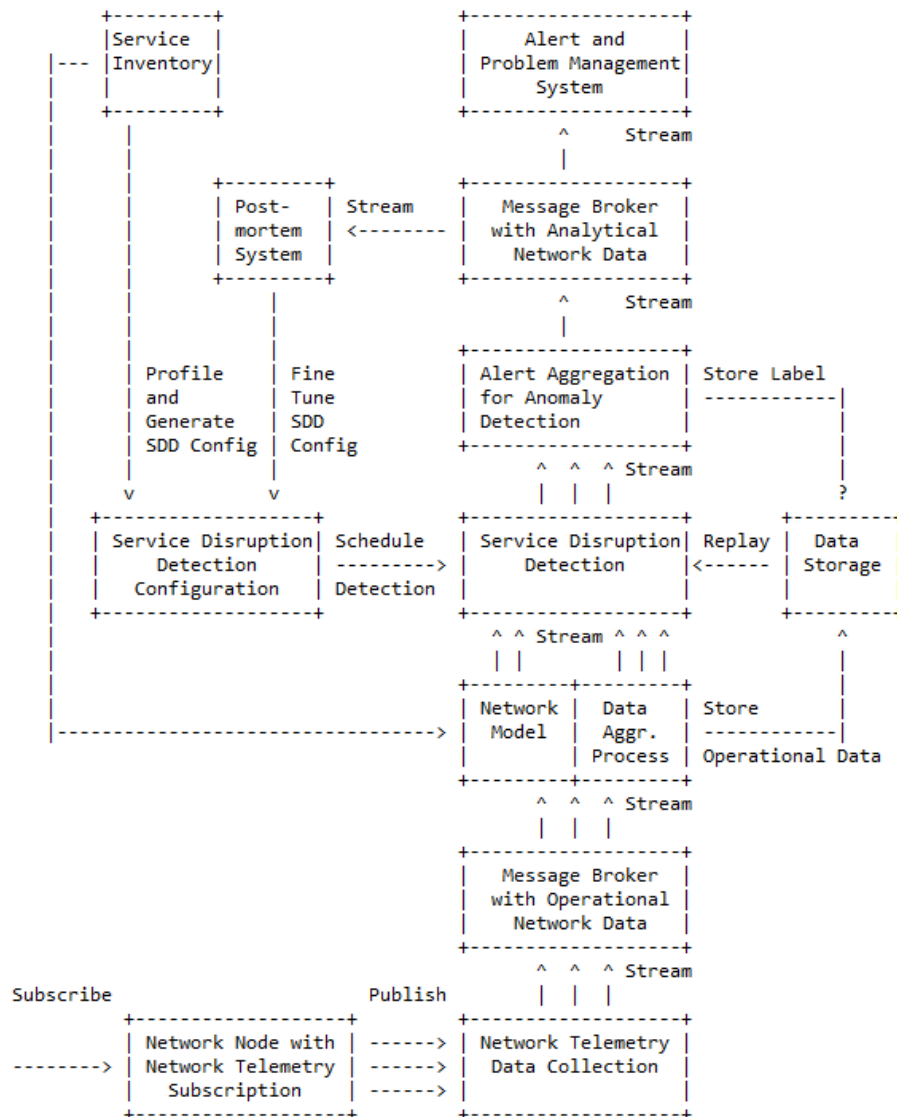
From network incidents postmortems we network operators **learn and improve** so does network anomaly detection and supervised and semi-supervised machine learning.

The more network incidents are observed, the more we can improve. With more incidents the **postmortem process needs be automated, let's get organized** first by defining human and machine-readable metadata semantics and annotate operational and analytical data.

Let's get further organized by exchanging standardized labeled network incident data among network operators, vendors and academia to **collaborate on academic research**.

« The community working on Network Anomaly Detection is probably the only group wishing for more network incidents »

Elements of the Architecture



- **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.

Semantic Metadata Annotation for Network Anomaly Detection

draft-netana-nmop-network-anomaly-semantics

```
module: ietf-symptom-semantic-metadata
```

```
  +--rw symptom
```

```
    +--rw id?                yang:uuid
    +--rw event-id?          yang:uuid
    +--rw description?       string
    +--rw start-time?        yang:date-and-time
    +--rw end-time?          yang:date-and-time
    +--rw confidence-score?  score
    +--rw concern-score?    score
```

```
    +--rw tags* [key]
```

```
      | +--rw key   string
      | +--rw value string
```

```
    +--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 (annotator-type)
      | +--:(human)
      | | +--rw human          empty
      | +--:(algorithm)
      | | +--rw algorithm      empty
      +--rw name?             string
```

- **Symptom ID and description** uniquely identifies the detected anomaly. **Event ID, start/end-time and confidence/concern-score** uniquely identifies the network event with its start and end time, how confident the system identified the anomaly and how concerned an operator should be.
- **Tags** allows to add customer information.
- **Pattern** describes the identified pattern of the anomaly.
- **Annotator Name, Type**, describes wherever the anomaly was detected by a human or algorithm and uniquely identifies the system who/which detected.

Experiment: Network Anomaly Lifecycle

draft-netana-nmop-network-anomaly-lifecycle

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

4. Lifecycle of a Network Anomaly

The lifecycle of a network anomaly can be articulated in three phases, structured as a loop: Detection, Validation, Refinement.

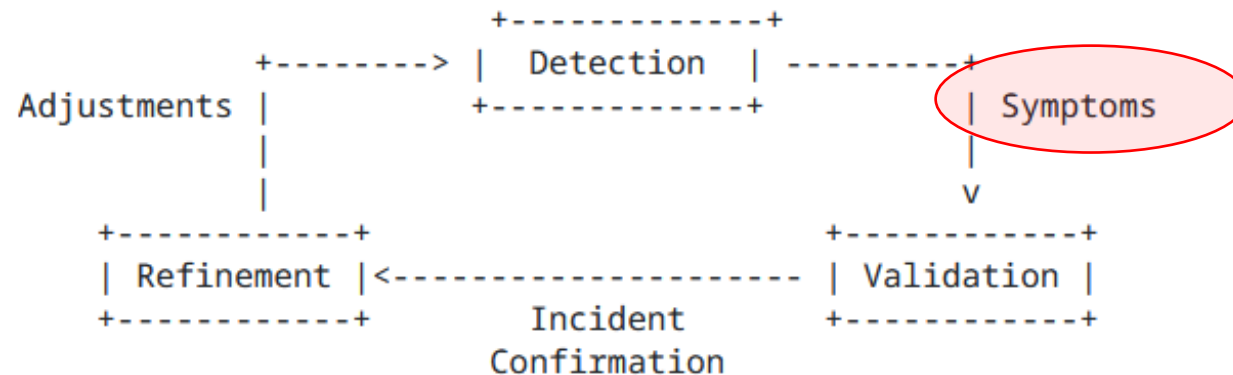


Figure 1: Anomaly Detection Refinement Lifecycle

Each of these phases can either be performed by a network expert or an algorithm or complementing each other.

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 operator performs detailed postmortem analysis of the network incident, collected Network Telemetry data and detected anomaly with the objective to identify useful adjustments in the Network Telemetry data collection and Anomaly Detection system.

Experiment: Network Anomaly Lifecycle

draft-netana-nmop-network-anomaly-lifecycle

```
module: ietf-network-anomaly-metadata
```

```
  +--rw network-anomalies
```

```
    +--rw network-anomaly* [id version]
```

```
      +--rw id                yang:uuid
```

```
      +--rw version           uint32
```

```
      +--rw description?      string
```

```
      +--rw state              identityref
```

```
      +--rw annotator
```

```
        | +--rw (annotator-type)
```

```
        | | +--:(human)
```

```
        | | | +--rw human          empty
```

```
        | | +--:(algorithm)
```

```
        | |   +--rw algorithm      empty
```

```
        | +--rw name?              empty
```

```
      +--rw symptoms* [symptom_id]
```

```
        +--rw symptom_id          yang:uuid
```

- **ID and Description** uniquely identifies the detected network anomaly (as a container of symptoms).
- **Description and State** provide general information regarding the anomaly and .
- **Annotator** describes the entity that observed the network anomaly: this can be a human or an algorithm (anomaly detection system).
- **Symptoms** provides a list of symptoms (based on ietf-symptom-metadata) that are part of this network anomaly.

Postmortem, L3 VPN Pilot Migration - Voice Over IP

Post Maintenance Window Analysis

<div> <div>FILTER</div> <div> <div>Apr 9, 23:33-23:55</div> <div>Ip Prefix: 138.187.57.24...</div> <div>Log Type: 2 values</div> <div>Rd: 4 values</div> <div>+2</div> <div>+</div> </div> </div>		<div> <div>SHOW</div> <div> <div>Time (5 Minutes)</div> <div>Log Type</div> <div>Rd</div> <div>Bgp Nexthop</div> <div>+2</div> <div>+</div> </div> </div>		Table
Time, Log Type, Rd, Bgp Nexthop, Platform Id, Node Id	Count			
Overall	48			
Apr 9, 23:30-23:35	36			
withdraw	36			
0:60633:4101214024	36			
138.187.57.5	36			
BNS_GW	36			
bc001ro0101ss	6			
bc001ro0101zhb	6			
bc001ro0101zhh	6			
bc001ro0101lss	6			
bc001ro0101zhb	6			
bc001ro011zhh	6			
Apr 9, 23:35-23:40	6			
withdraw	6			
0:60633:4101214024	6			
138.187.57.5	6			
BNS_GW	6			
bc001ro011olt	6			
Apr 9, 23:50-23:55	6			
withdraw	6			
0:60633:4101214024	6			
138.187.57.5	6			
BNS_GW	6			
bc001ro0101olt	6			

Overall BGP Update/withdrawals Across Swisscom MPLS/SRv6 Cores



Maintenance window was scheduled to start on April 9th 22:00 with a total of 4 migration steps.



At 12:45 CE facing interfaces on first PE **node to be phased out was disabled.**

Triggering a VPNv4 withdrawal of 138.187.57.240/28 from 138.187.57.6 Lo0 towards route-reflectors and then to Inter-AS Option B ASBR. BMP route-monitoring and CLI show commands verified successful route propagation.



At 23:02 CE facing interfaces on first PE **node to be migrated to was enabled.**

Triggering a VPNv4 update of 138.187.57.240/28 from 138.190.129.180 Lo0 towards route-reflectors and then to Inter-AS option B ASBR. BMP route-monitoring and CLI show commands verified successful route propagation.



At 23:34 CE facing interfaces on second PE **node to be phased out was disabled.**

Triggering a VPNv4 withdrawal of 138.187.57.240/28 from 138.187.57.5 Lo0 towards route-reflectors and then to Inter-AS option B ASBR. BMP route-monitoring and CLI show commands verified successful route propagation to route-reflector **and on two Option B ASBR, but on other six after 20 mins delay.**

Postmortem, L3 VPN Pilot Migration - Voice Over IP

Show command drove to wrong conclusion

```
show route table bgp.l3vpn.0 protocol bgp 138.187.57.240/28 detail
```

```
60633:4101214024:138.187.57.240/28 (1 entry, 1 announced)
  BGP      Preference: 170/-101
           Route Distinguisher: 60633:4101214024
           Next hop type: Indirect, Next hop index: 0
           Address: 0x1a963a3c
           Next-hop reference count: 8
           Source: 138.190.128.116
           Protocol next hop: 138.187.57.5
           Label operation: Push 83714
           Label TTL action: prop-ttl
           Load balance label: Label 83714: None;
           Indirect next hop: 0x2 no-forward INH Session ID: 0x0
           State: <Delete Int Ext ProtectionPath ProtectionCand>
           Local AS: 64088.1116 Peer AS: 64088.1116
           Age: 5:28      Metric: 805      Metric2: 4
           Validation State: unverified
           Resolving-AIGP: 4
           Effective metric: 8 (IGP metric plus resolving AIGP)
           Task: BGP_64088.1116.138.190.128.116
           Announcement bits (1): 1-BMP
           AS path: 60633 64088.5 ?
           Communities: 60633:204 60633:208 60633:1002 64497:4965
64499:13338 target:60633:1100006314
  Accepted
  BMP: Pre: withdraw Station: DAISY_BMP_1
  BMP: Pre: withdraw Station: DAISY_BMP_2
  BMP: Station: <unassigned>
           Color: VPN Label: 83714
  Localpref: 100
  Router ID: 138.190.128.116
  Thread: junos-main
```

```
show route table bgp.l3vpn.0 protocol bgp 138.187.57.240/28 detail
```

```
60633:4103214024:138.187.57.240/28 (3 entries, 1 announced)
  *BGP     Preference: 170/-101
           Route Distinguisher: 60633:4103214024
           Next hop type: Indirect, Next hop index: 0
           Address: 0x1526757c
           Next-hop reference count: 4
           Source: 138.187.57.3
           Protocol next hop: 138.190.128.180
           Label operation: Push 83118
           Label TTL action: prop-ttl
           Load balance label: Label 83118: None;
           Indirect next hop: 0x2 no-forward INH Session ID: 0x0
           State: <Active Ext ProtectionPath ProtectionCand>
           Local AS: 64088.1116 Peer AS: 60633
           Age: 14:29:45      Metric: 800      Metric2: 4
           Validation State: unverified
           Resolving-AIGP: 4
           Effective metric: 8 (IGP metric plus resolving AIGP)
           Task: BGP_60633.138.187.57.3
           Announcement bits (2): 0-BGP_RT_Background 1-BMP
           AS path: 60633 64088.1180 ?
           Communities: 60633:204 60633:208 60633:1001 60633:1111
64497:4965 64499:13338 target:60633:1100006314
  Accepted
  BMP: Pre: advertise Station: DAISY_BMP_1
  BMP: Pre: advertise Station: DAISY_BMP_2
           Color: VPN Label: 83118
  Localpref: 100
  Router ID: 138.187.57.3
  Thread: junos-main
```



Juniper JunOS
CLI show
command
shows that path
is for 20min no
longer primary
active but still
as backup path
inactive. **Output
mislead
network
engineer to
believe that
path is still
installed.**

Postmortem, L3 VPN Pilot Migration - Voice Over IP

Data collection timestamp drove to wrong conclusion

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "bew03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.190.128.117",  
"string": "Tue Apr 09 2024 23:52:34"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "bew03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.187.57.4",  
"string": "Tue Apr 09 2024 23:52:34"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "bew03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.187.57.3",  
"string": "Tue Apr 09 2024 23:52:34"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "bew03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.190.128.117",  
"string": "Wed Apr 10 2024 01:04:00"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "zoi03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.187.57.3",  
"string": "Tue Apr 09 2024 23:54:09"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "zoi03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.187.57.4",  
"string": "Tue Apr 09 2024 23:54:17"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "zoi03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.190.128.117",  
"string": "Tue Apr 09 2024 23:54:24"
```

```
"timestamp": "Tue Apr 09 2024 23:34:21",  
"writer_id": "zoi03bmp45c 20240220-1 (45ae4201)",  
"peer_ip": "138.190.128.117",  
"string": "Wed Apr 10 2024 00:54:51"
```

The yellow marked timestamp shows the optional BMP per-peer header observation timestamp.

The blue marked timestamp shows the timestamp being augmented on the BMP data collection and **being used for the time series database.**



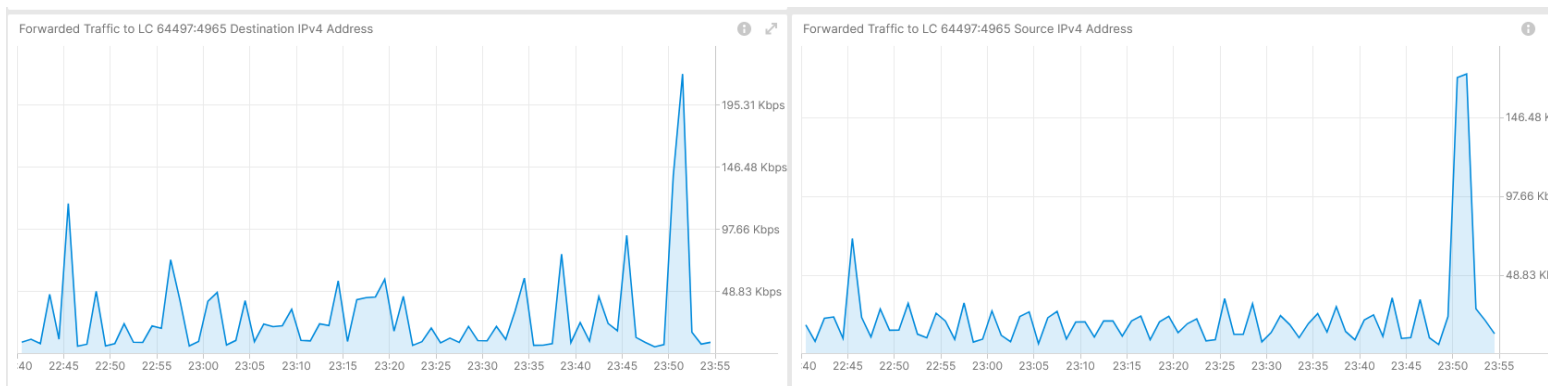
Because BMP per-peer timestamp is optional, in the time series database ingestion, the data collection augmentation timestamp is used instead. **Leading to false conclusions when the state change was observed.**

Postmortem, L3 VPN Pilot Migration - Voice Over IP

Route-Reflector Peering and L3 VPN Traffic View



BMP Peering Statistics on Route Reflectors



Traffic to Voice over IP Service on affected L3 VPN



IPFIX configured on PE
**but not on involved
MPLS Inter-AS option B
ASBRs due to
PR1567039.**



BMP ADJ-RIB In pre-policy on BGP VPNv4 /6 on MPLS PE's. BMP ADJ-RIB In pre-policy on BGP VPNv4 /6 on Route Reflectors and BMP ADJ-RIB In pre-policy and ADJ-RIB Out post-policy on Inter-AS Option B ASBR.



YANG Push on most nodes but not relevant for this use case.

Postmortem, L3 VPN Pilot Migration - Voice Over IP

64497:4965 - Anomaly Detection - Live

Max Concern Score: **NA**
BMP Withdrawal Score: **0.19**



BMP route-monitoring
Update/Withdraw check recognize withdrawal.



BMP peer Down/Up check did not apply.



Interface Down/Up check did not recognize.



Traffic Drop spike did not apply.



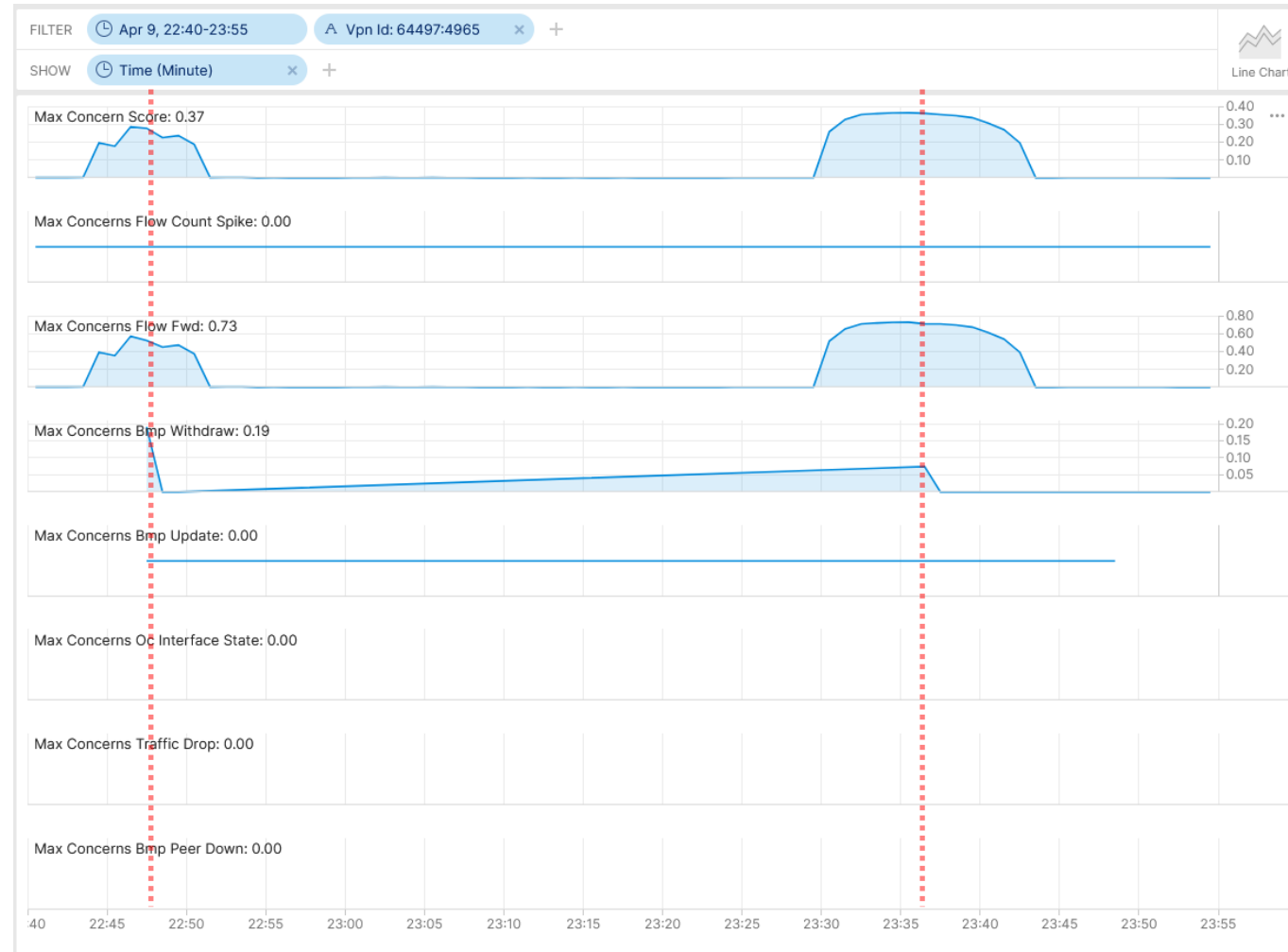
Missing Traffic check did not apply.
(not fully implemented yet).



Increased or decreased Flow Count did not apply.



Overall: 1 out of 6 checks have detected the BGP topology change.
Real-time streaming implementation work in progress as expected.



Postmortem

What to do next?

- **Support on upcoming maintenance window with verification dashboard and active monitoring.**
-> Done

What went well?



Work in progress Cosmos Bright Lights real-time streaming Anomaly Detection BMP route-monitoring withdrawal rule detected topology change.



BMP collected metrics are consistent across multiple vendors vs. CLI show output is vendor dependent.

What could be improved?



BMP per-peer observation timestamp should be mandatory. See <https://datatracker.ietf.org/doc/html/draft-boucadair-nmop-rfc3535-20years-later-02#section-4.7>. -> **To be addressed in GROW/NMOP.**

BMP per-peer header should have an export timestamp. See <https://datatracker.ietf.org/doc/html/draft-boucadair-nmop-rfc3535-20years-later-02#section-4.7>. -> **To be addressed in GROW/NMOP.**

With [RFC 8671](#) (Support for Adj-RIB-Out in BMP) path propagation could have been observed on route-reflectors.

With [draft-lucente-grow-bmp-rel](#) (Logging of routing events in BMP) path drops could be observed on Inter-AS option B ASBRs and route-reflectors.

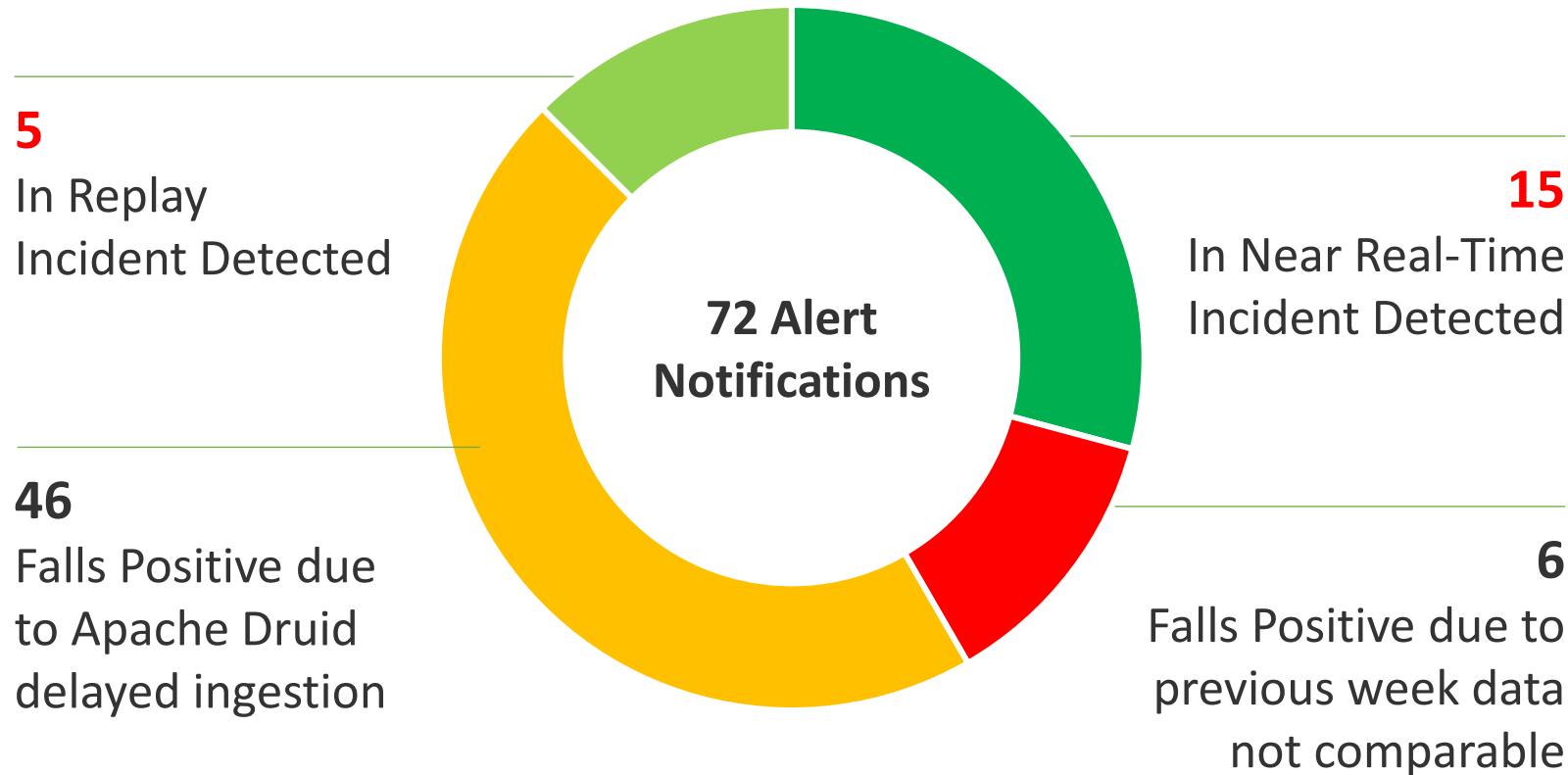
With [draft-ietf-grow-bmp-path-marking-tlv](#) path status changed could have been observed on Inter-AS option B ASBRs.

Clarify why Juniper JunOS delayed BMP export for 20 resp. 80 minutes. Due to fact that the path was still passive in the BGP RIB?

With IPFIX (**deconfigured due to PR1567039**) and support of IE90 ForwardingStatus (**not supported on Juniper JunOS**) forwarding drops could have been observed on Inter-AS option B ASBRs.

Swisscom - Cosmos Bright Lights PoC Summary

After 20 Incidents and 18 Months Time

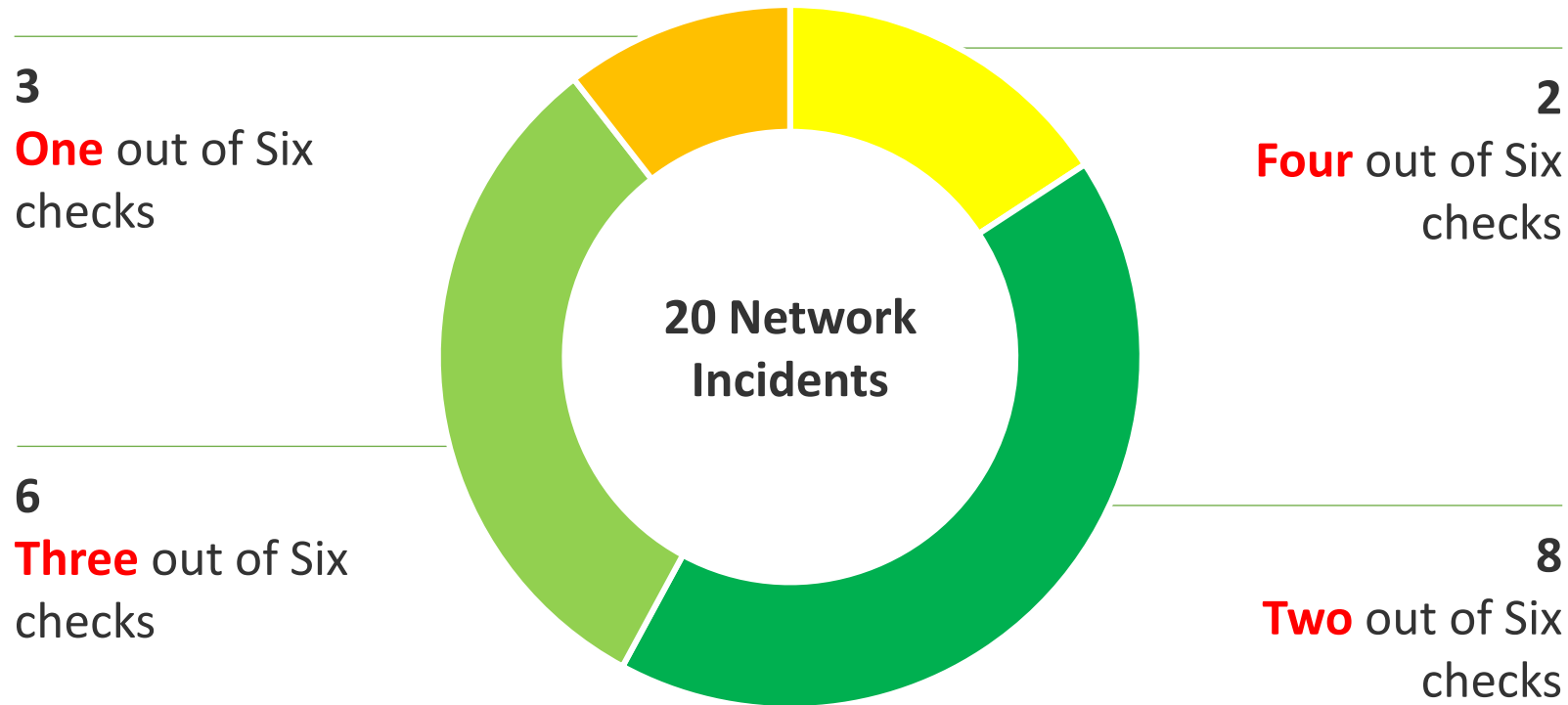


Key Facts in V0 (2023-2024)

- 16 L3 VPNs proactively monitored.
- Individual Service Disruption Detection rule accuracy is beyond 90%. Summed accuracy is beyond 95%.
- Max Concern score ranged between 0.06 and 0.85. In average 0.46.
- In 4 cases additional YANG, in 13 cases additional BMP, in 2 cases Netconf Transaction-ID and 1 case additional L2 IPFIX metrics would have helped to gain more visibility.
- Key observability feature missing: BMP Local RIB with Path Marking.

Swisscom - Cosmos Bright Lights PoC Detail

Multiple Perspectives increases Accuracy



Key Improvements in V1 (2024)

- >12000 L3 VPNs proactively monitored since June 2024.
- Realtime Streaming eliminates delayed ingestion falls positives and scaling.
- Improved profiling. Compares to multiple previous weeks and discard largest deviation eliminates falls positives.
-> Work In progress

Key Improvements in V2 (2025)

- Annotate operational and analytical Network Incident data for reproduction.
- Enabling automated workflow. From PowerPoint slide decks to data driven actionable insights.

Network Anomaly Detection Framework

Detect service interruption faster than humans can

Incident and Problem Management:

- Some Key Terms for Network Incident and Problem Management

[draft-ietf-nmop-terminology](#)



Network Anomaly Detection:

- An Architecture for a Network Anomaly Detection Framework

[draft-netana-nmop-network-anomaly-architecture](#)



- Semantic Metadata Annotation for Network Anomaly Detection

[draft-netana-nmop-network-anomaly-semantics](#)



- Experiment: Network Anomaly Lifecycle

[draft-netana-nmop-network-anomaly-lifecycle](#)



« Addressing the need to detect connectivity service interruption faster than humans can and facilitate collaboration by enabling exchange on labeled data with standardized semantics on a common framework.

Please consider to attend IETF 120 NMOP working group session on Friday 13:00 – 15:00 or go onto the mailing list and contribute to the discussion. »

Relevant Papers for more Details

Practical Anomaly Detection in Internet Services: An ISP centric approach

Alex Huang Feng*, Pierre Francois*, Kensuke Fukuda†, Wanting Du†, Thomas Graf †, Paolo Lucente§, Stéphane Frénot*

*INSA Lyon, ‡National Institute of Informatics, †Swisscom, §pmacct.net

alex.huang-feng@insa-lyon.fr, pierre.francois@insa-lyon.fr, kensuke@nii.ac.jp, wanting.du@swisscom.com, thomas.graf@swisscom.com, paolo@pmacct.net, stephane.frenot@insa-lyon.fr

Context

- ISPs provide multiple **IP connectivity services** such as:
 - BGP/MPLS VPNs
 - Internet Connectivity
- Network **disruptions and anomalies** degrade the reputation and impact the business of ISPs
- Network operators want to detect these anomalies
 - Comprehensively**: to understand the issue when alerted
 - Automatically**: to provide a notification if possible
- How can we detect these anomalies in **real world ISPs**?
- Which data can we use? Can we use **Shodan** only?
- Can a **rule-based approach** leveraging knowledge from operations be effective?

Challenges of ISP networks

- Real world networks are heterogeneous:
 - Built with devices from multiple vendors
 - Devices have different network telemetry capabilities
 - Devices could not all be monitored
- State of the art focused mostly on:
 - Internet topology using BGP
 - Public data (Routefviews & RIPE NCC Archives)
 - Very few using production data & detecting anomalies in a single domain [1–3]

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

accepted at AnNet’24

(in conjunction with IEEE NOMS’24)

Seoul, Korea (6–10 May 2024)

[Will be presented as a poster the May 6th 2024]

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

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

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

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

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

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.

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.

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, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

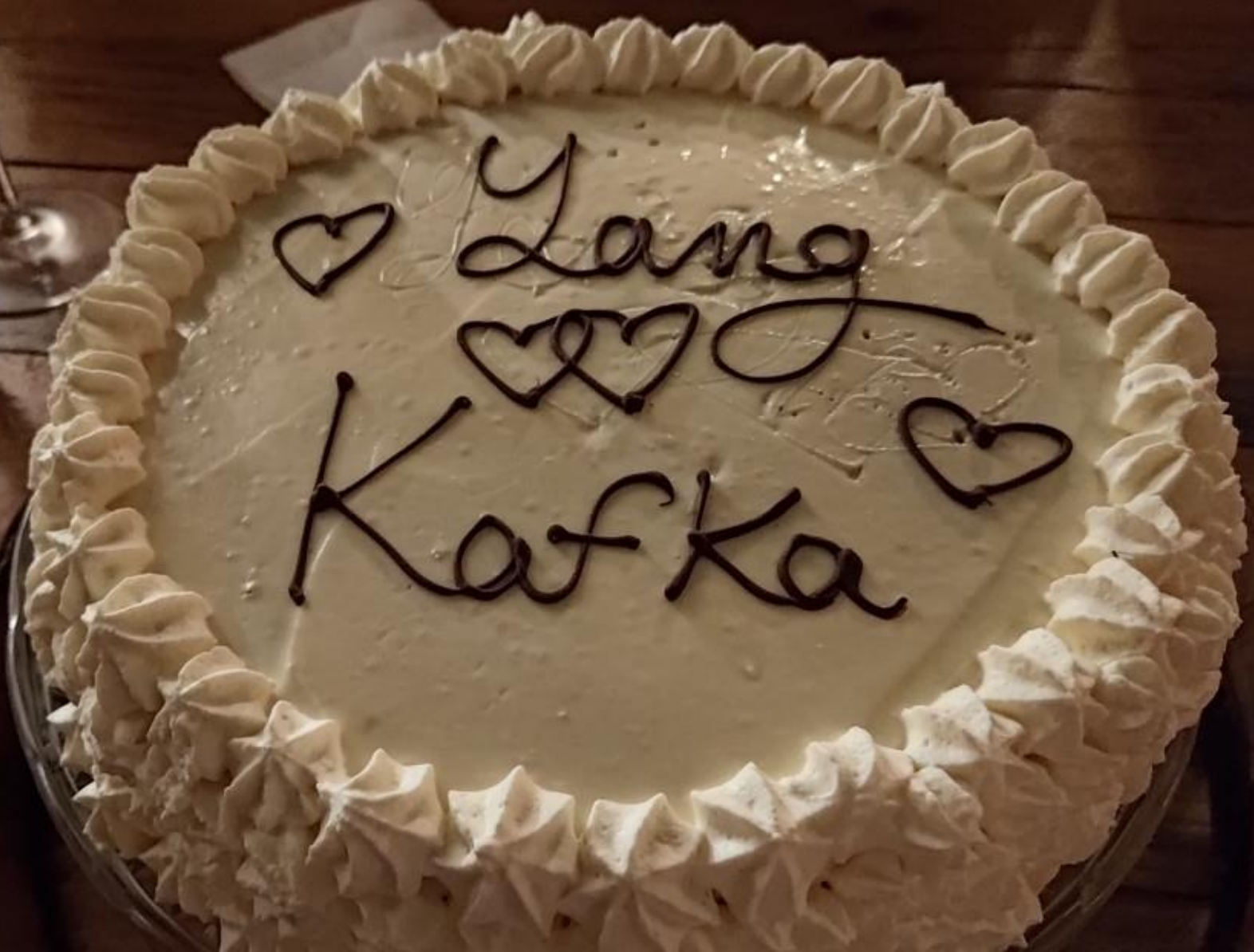
ANRW '23, July 24, 2023, San Francisco, CA, USA
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-4-4007-0274-7/23/007...\$15.00
<https://doi.org/10.1145/3606464.3606470>

Paper “**Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks**”

published at ACM/IRTTF ANRW’23

San Francisco, USA (24 July 2023)

Open access: <http://hal.science/hal-04307611>



♥ Yang ♥♥♥
Kafka ♥

Handling Operational YANG Modelled Data

State of the Union

Nowadays network operators are using **machine and human readable YANG** [RFC 7950](#) to model their configurations and obtain YANG modelled data from their networks.

Network operators organizing their data in a Data Mesh where a message broker such as Apache Kafka facilitates the exchange of messages among data processing components.

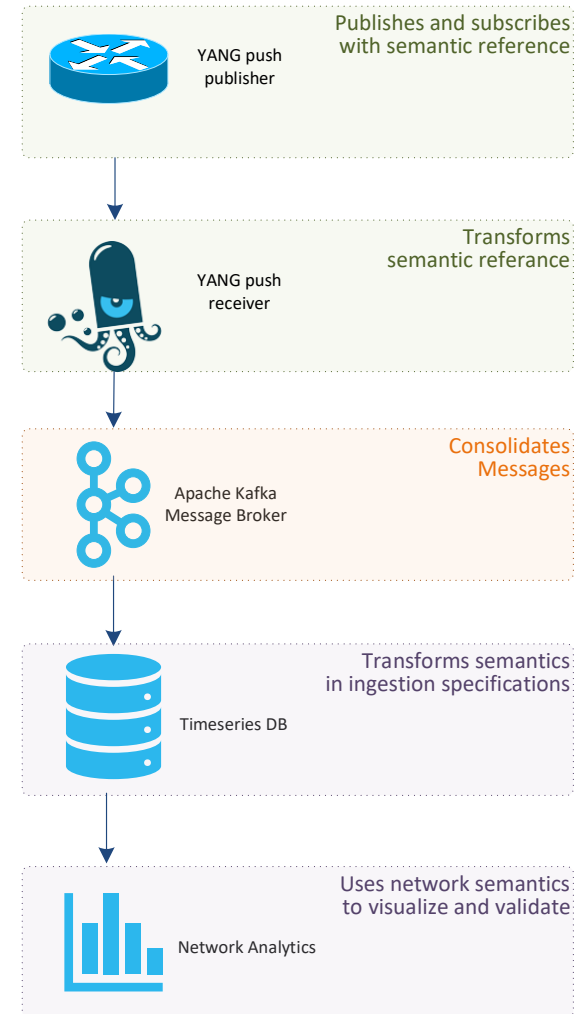
Today, subscribing to a YANG datastore, publishing a YANG modeled notifications message from the network and viewing the data in a time series database, **manual labor is needed to perform data transformation** to make a message broker and its data processing components with YANG notifications interoperable.

« Even though YANG is intend to ease the handling of data, **this promise has not yet been fulfilled** for Network Telemetry [RFC 9232](#) »

From YANG-Push to Network Analytics

Aiming for an automated data processing pipeline

- **A network operator aims for:**
 - An **automated data processing pipeline** which starts with YANG-Push, consolidates at Data Mesh and ends at Network Analytics.
 - Operational metrics where **IETF defines the semantics.**
 - Analytical metrics where **network operators gain actionable insights.**
- **We achieve this by integrating YANG-Push into Data Mesh to:**
 - Produce metrics from networks **with timestamps when network events were observed.**
 - Hostname, publisher ID and sequence numbers help us to understand **from where metrics were exported and measure its delay and loss.**
 - Forward **metrics unchanged** from networks
 - **Learn semantics** from networks and validate messages.
 - **Control semantic** changes end to end.



Elements of the Architecture

Workflow Diagram

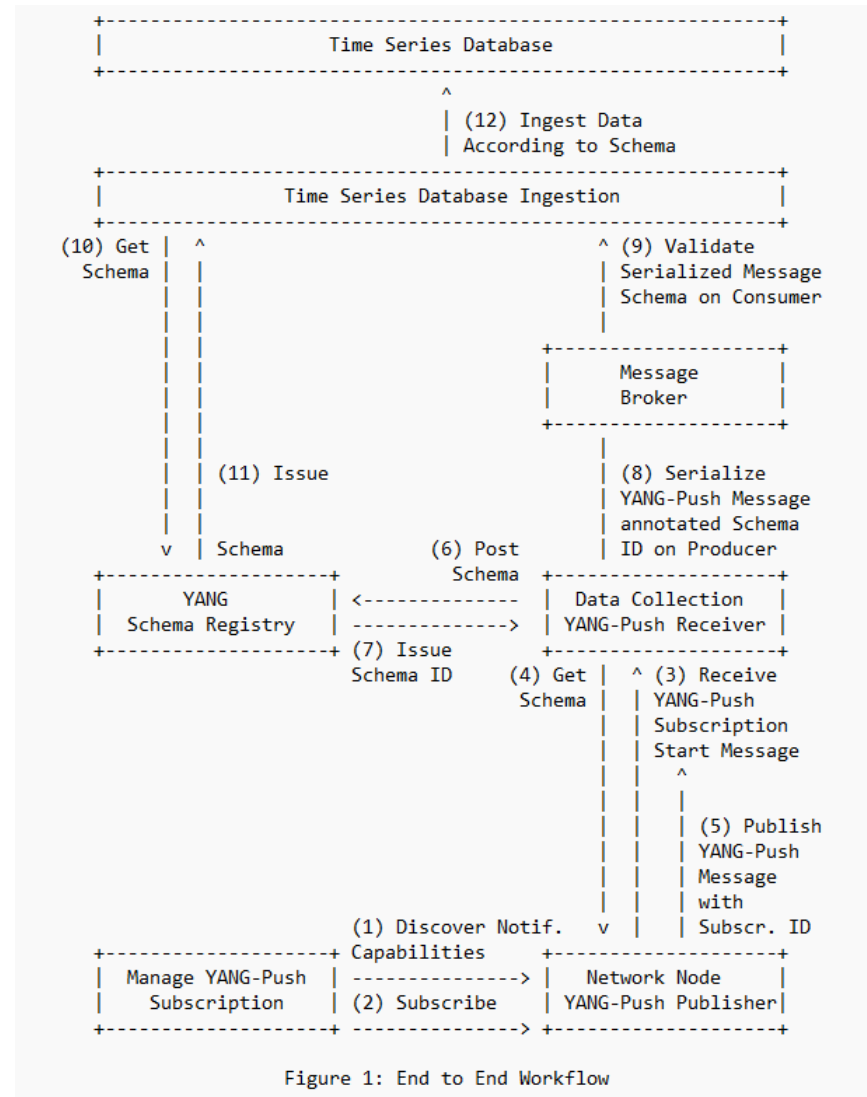


Figure 1: End to End Workflow

- **Network Orchestration** subscribes to YANG datastore.
- **Network Node** informs Data Collection on subscription state and publishes YANG metrics with YANG-Push.
- **Data Collection** obtains for each subscription the YANG module dependencies and the YANG modules on the network node, registers it in the YANG Schema Registry and prefixes the forwarded YANG notifications with the obtained schema ID.
- **YANG Schema Registry** issues for a Message Broker subject a schema ID for each new schema tree, compares a new schema tree with an existing and versions it.
- **Time Series Database Ingestion** consumes YANG-Push notifications from Message Broker, obtains schema tree from YANG schema registry, validates YANG notifications against schema and uses schema to populate into database table.

Address YANG Specification and Integration Gaps

Aiming for an automated data processing pipeline

YANG Specifications Gaps:

- YANG model for NETCONF Event Notifications

[draft-ahuang-netconf-notif-yang](#)



- Validating anydata in YANG Library context

[draft-aelhassany-anydata-validation](#)



YANG Integration Gaps:

- Support of Network Observation Timestamping in YANG Notifications

[draft-tgraf-netconf-yang-push-observation-time](#)



- Support of Hostname and Sequencing in YANG Notifications

[draft-tgraf-netconf-notif-sequencing](#)



- Support of Versioning in YANG Notifications Subscription

[draft-ietf-netconf-yang-notifications-versioning](#)



- Augmented-by Addition into the IETF-YANG-Library

[draft-linclanetconf-yang-library-augmentation](#)



« Addressing those gaps are a prerequisite to enable an automated data processing chain as described in [draft-ietf-nmop-yang-message-broker-integration](#).

Please consider to attend IETF 120 NMOP working group session on Friday 13:00 – 15:00 or go onto the mailing list and contribute to the discussion. »