An Architecture for a Network Anomaly Detection Framework

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

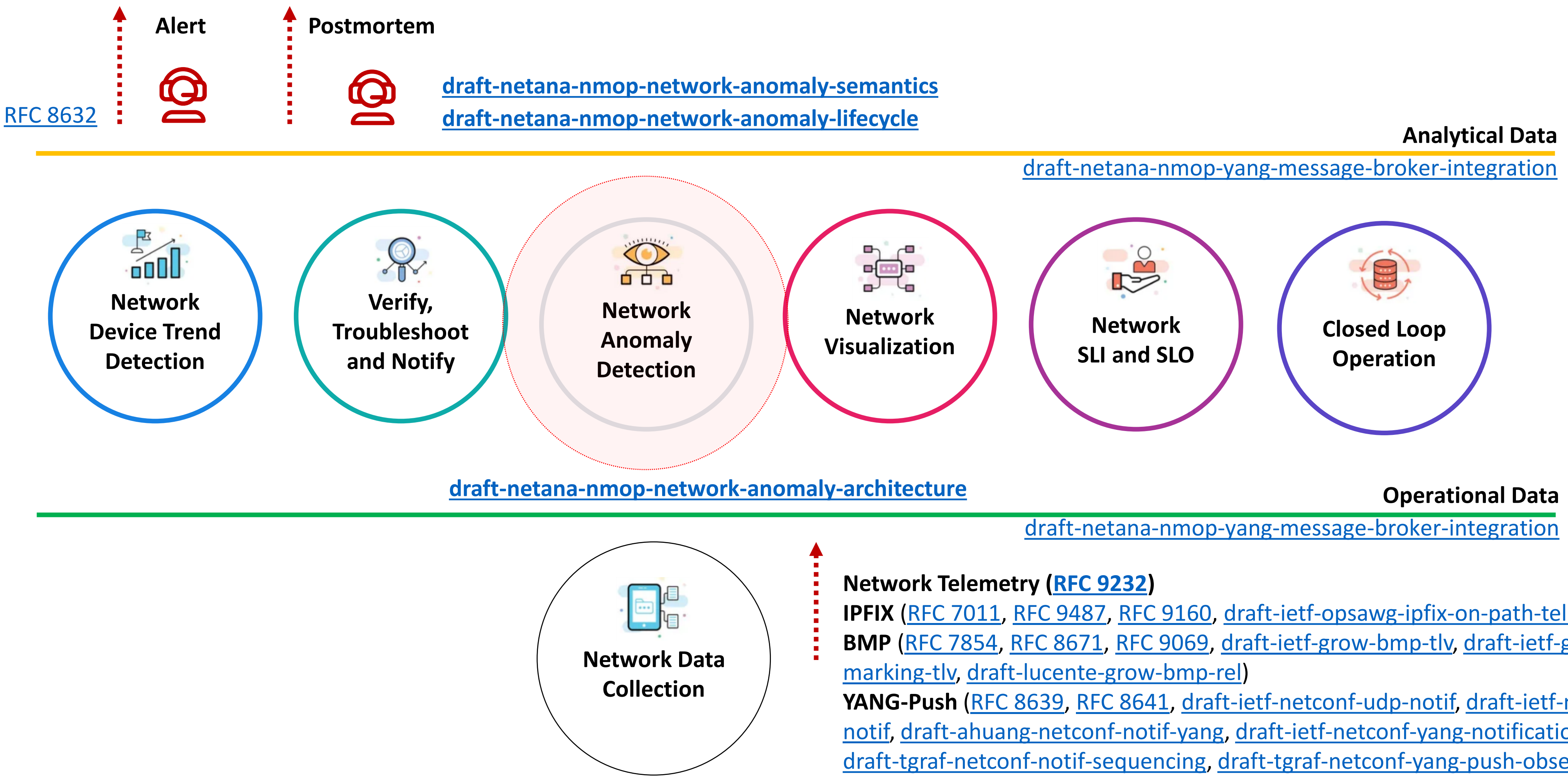
Motivation and architecture of a Network Anomaly Detection Framework
and the relationships to other documents describing
network symptom semantics and network incident lifecycle

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

25. July 2024

Data Mesh organizes Data in Organizations

Enables Network Analytics use cases



Alert
Postmortem
RFC 8632
draft-netana-nmop-network-anomaly-semantics
draft-netana-nmop-network-anomaly-lifecycle
Analytical Data
draft-netana-nmop-yang-message-broker-integration
Network Device Trend Detection
Verify, Troubleshoot and Notify
Network Anomaly Detection
Network Visualization
Network SLI and SLO
Closed Loop Operation
draft-netana-nmop-network-anomaly-architecture
Operational Data
draft-netana-nmop-yang-message-broker-integration
Network Data Collection

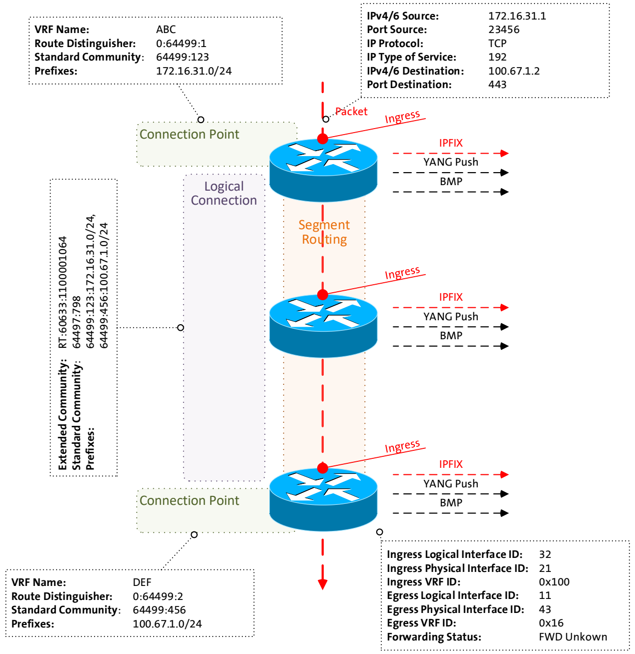
Network Telemetry (RFC 9232)
IPFIX (RFC 7011, RFC 9487, RFC 9160, draft-ietf-opsawg-ipfix-on-path-telemetry)
BMP (RFC 7854, RFC 8671, RFC 9069, draft-ietf-grow-bmp-tlv, draft-ietf-grow-bmp-path-marking-tlv, draft-lucente-grow-bmp-rel)
YANG-Push (RFC 8639, RFC 8641, draft-ietf-netconf-udp-notif, draft-ietf-netconf-distributed-notif, draft-ahuang-netconf-notif-yang, draft-ietf-netconf-yang-notifications-versioning, draft-tgraf-netconf-notif-sequencing, draft-tgraf-netconf-yang-push-observation-time)

What to monitor

Which 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 »



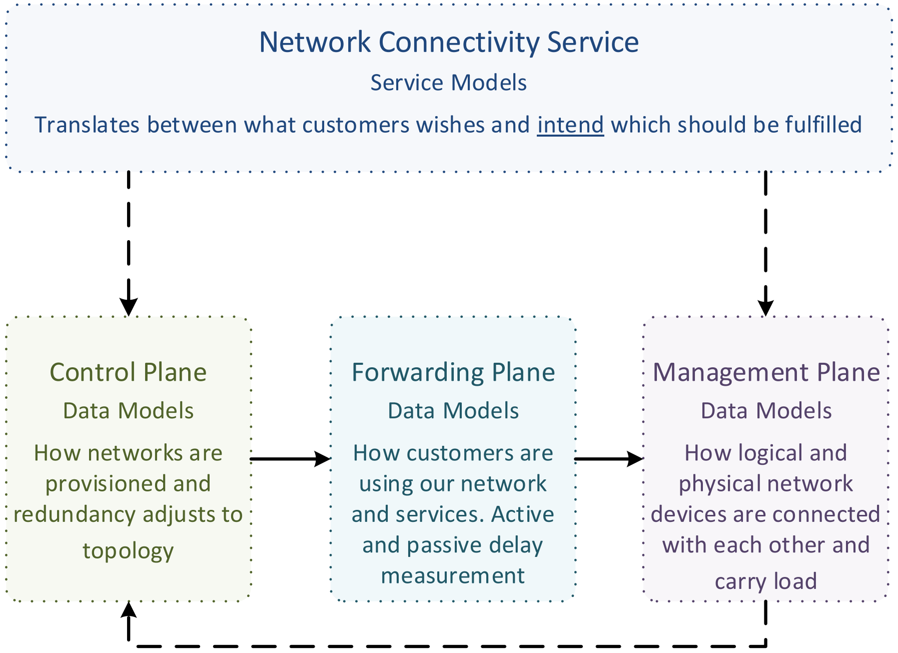
VRF Name:	ABC
Route Distinguisher:	0:64499:1
Standard Community:	64499:123
Prefixes:	172.16.31.0/24

IPv4/6 Source:	172.16.31.1
Port Source:	23456
IP Protocol:	TCP
IP Type of Service:	192
IPv4/6 Destination:	100.67.1.2
Port Destination:	443

Extended Community:	RT:60633:1100001064
Standard Community:	64497:798
Prefixes:	64499:123:172.16.31.0/24, 64499:456:100.67.1.0/24

VRF Name:	DEF
Route Distinguisher:	0:64499:2
Standard Community:	64499:456
Prefixes:	100.67.1.0/24

Ingress Logical Interface ID:	32
Ingress Physical Interface ID:	21
Ingress VRF ID:	0x100
Egress Logical Interface ID:	11
Egress Physical Interface ID:	43
Egress VRF ID:	0x16
Forwarding Status:	FWD Unkown



Network Connectivity Service

Service Models

Translates between what customers wishes and intend which should be fulfilled

Control Plane

Data Models

How networks are provisioned and redundancy adjusts to topology

Forwarding Plane

Data Models

How customers are using our network and services. Active and passive delay measurement

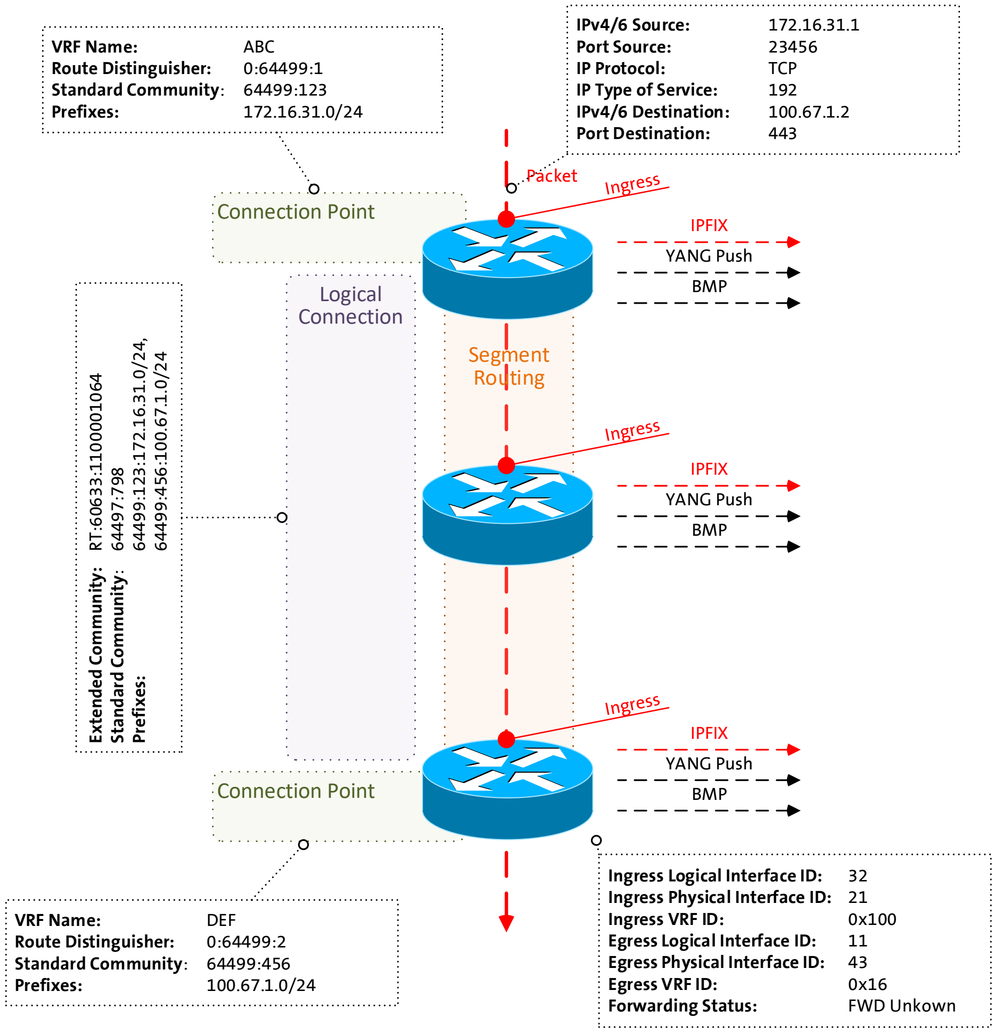
Management Plane

Data Models

How logical and physical network devices are connected with each other and carry load

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

From Connectivity Service to Realtime Network Analytics



VRF Name:	ABC
Route Distinguisher:	0:64499:1
Standard Community:	64499:123
Prefixes:	172.16.31.0/24

IPv4/6 Source:	172.16.31.1
Port Source:	23456
IP Protocol:	TCP
IP Type of Service:	192
IPv4/6 Destination:	100.67.1.2
Port Destination:	443

Extended Community:	RT:60633:1100001064
Standard Community:	64497:798
Prefixes:	64499:123:172.16.31.0/24, 64499:456:100.67.1.0/24

VRF Name:	DEF
Route Distinguisher:	0:64499:2
Standard Community:	64499:456
Prefixes:	100.67.1.0/24

Ingress Logical Interface ID:	32
Ingress Physical Interface ID:	21
Ingress VRF ID:	0x100
Egress Logical Interface ID:	11
Egress Physical Interface ID:	43
Egress VRF ID:	0x16
Forwarding Status:	FWD Unkown

- **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.

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

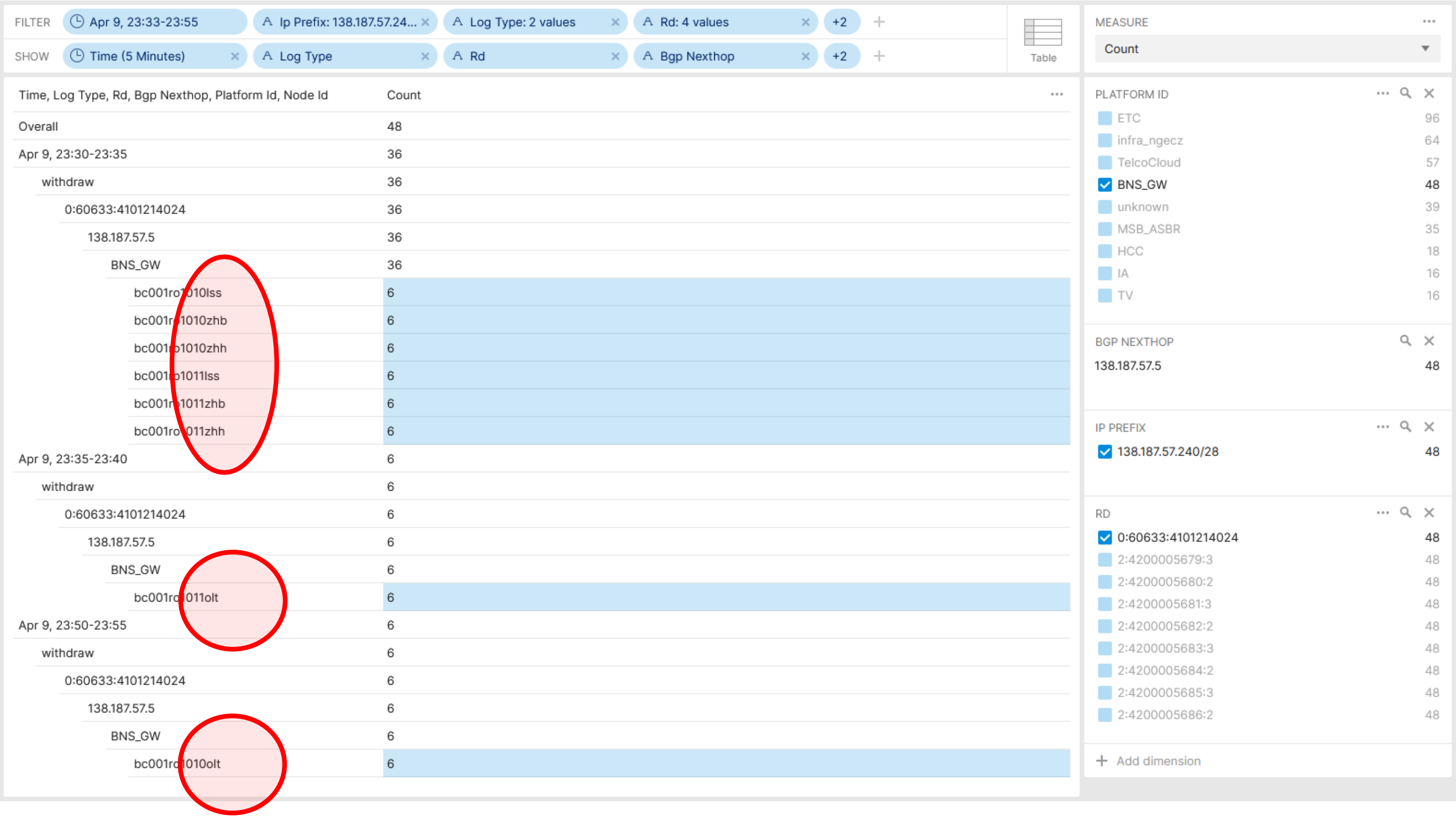
Consumes operational real-time Forwarding Plane, Control Plane and Management Plane metrics and produces analytical alerts.

Direction

From connectivity service to network platform.

Postmortem, L3 VPN Pilot Migration - Voice Over IP

Post Maintenance Window Analysis



FILTER: Apr 9, 23:33-23:55 · Ip Prefix: 138.187.57.24... · Log Type: 2 values · Rd: 4 values · +2

SHOW: Time (5 Minutes) · Log Type · Rd · Bgp Nexthop · +2

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
bc001ro1010lss	6
bc001ro1010zhb	6
bc001ro1010zhh	6
bc001ro1011lss	6
bc001ro1011zhb	6
bc001ro1011zhh	6
Apr 9, 23:35-23:40	6
withdraw	6
0:60633:4101214024	6
138.187.57.5	6
BNS_GW	6
bc001ro1011olt	6
Apr 9, 23:50-23:55	6
withdraw	6
0:60633:4101214024	6
138.187.57.5	6
BNS_GW	6
bc001ro1010olt	6

MEASURE: Count

PLATFORM ID	
□ ETC	96
□ infra_ngecz	64
□ TelcoCloud	57
☑ BNS_GW	48
□ unknown	39
□ MSB_ASBR	35
□ HCC	18
□ IA	16
□ TV	16

BGP NEXTHOP	
138.187.57.5	48

IP PREFIX	
☑ 138.187.57.240/28	48

RD	
☑ 0:60633:4101214024	48
□ 2:4200005679:3	48
□ 2:4200005680:2	48
□ 2:4200005681:3	48
□ 2:4200005682:2	48
□ 2:4200005683:3	48
□ 2:4200005684:2	48
□ 2:4200005685:3	48
□ 2:4200005686:2	48

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.

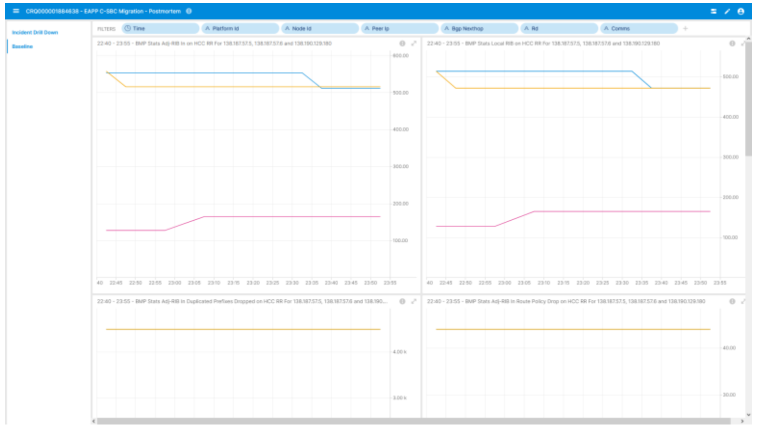
The blue marked timestamp shows the timestamp being augmented on the BMP data collection and **being used for the time series database.**

SOS

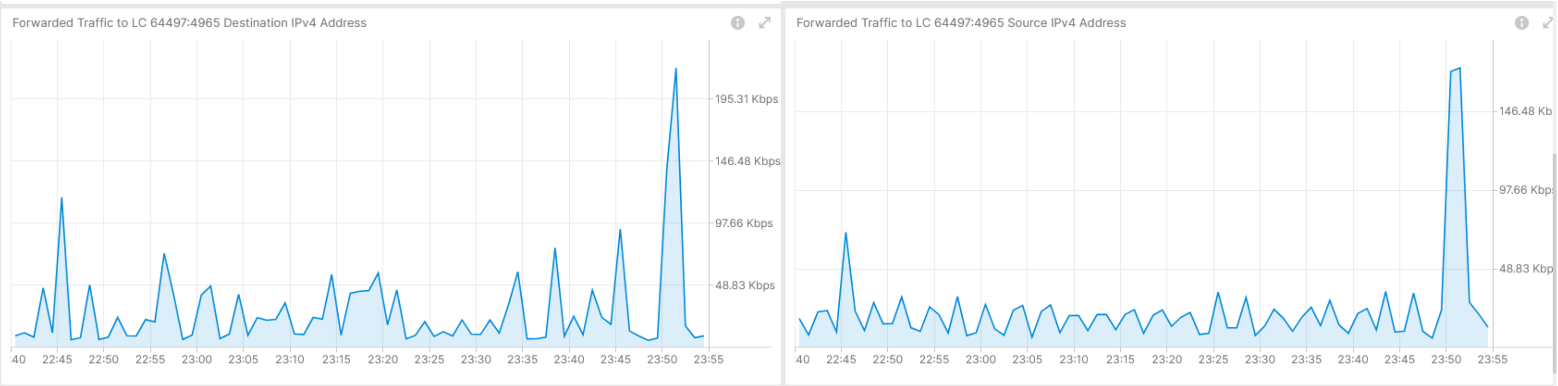
Because BMP per-peer timestamp is optional, in the time series database ingestion, the data collection augmentation timestamp is used instead. **Leading to false conclusions when the state change was observed.**

Postmortem, L3 VPN Pilot Migration - Voice Over IP

Route-Reflector Peering and L3 VPN Traffic View


CRQ000001884638 - EAPP C-SBC Migration - Postmortem
Incident Drill Down
Baseline
FILTERS
Time
Platform Id
Node Id
Peer Ip
Bgp Nexthop
Rd
Comms
22:40 - 23:55 - BMP Stats Adj-RIB In on HCC RR For 138.187.57.5, 138.187.57.6 and 138.190.129.180
22:40 - 23:55 - BMP Stats Local RIB on HCC RR For 138.187.57.5, 138.187.57.6 and 138.190.129.180
22:40 - 23:55 - BMP Stats Adj-RIB In Duplicated Prefixes Dropped on HCC RR For 138.187.57.5, 138.187.57.6 and 138.190....
22:40 - 23:55 - BMP Stats Adj-RIB In Route Policy Drop on HCC RR For 138.187.57.5, 138.187.57.6 and 138.190.129.180
600.00
500.00
400.00
100.00
4.00 k
40.00
40
22:45
22:50
22:55
23:00
23:05
23:10
23:15
23:20
23:25
23:30
23:35
23:40
23:45
23:50
23:55

BMP Peering Statistics on Route Reflectors



Traffic to Voice over IP Service on affected L3 VPN

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

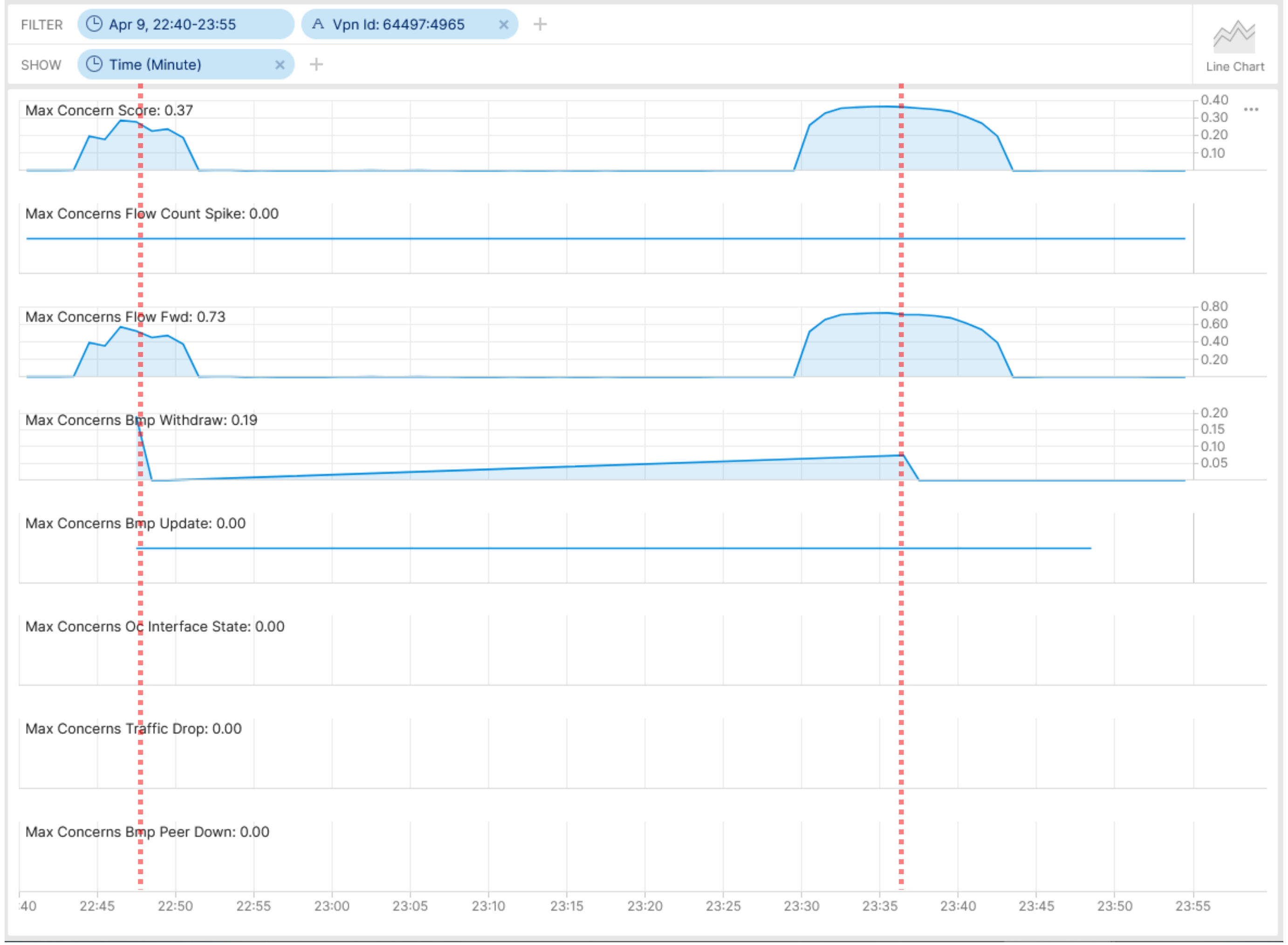
BMP ADJ-RIB In pre-policy on BGP VPNv4 /6 on MPLS PE's. BMP ADJ-RIB In pre-policy on BGP VPNv4 /6 on Route Reflectors and BMP ADJ-RIB In pre-policy and ADJ-RIB Out post-policy on Inter-AS Option B ASBR.

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

Real-Time Streaming
under Development

Postmortem, L3 VPN Pilot Migration - Voice Over IP

64497:4965 - Anomaly Detection - Live



FILTER Apr 9, 22:40-23:55 | Vpn Id: 64497:4965

SHOW Time (Minute)

Line Chart
Max Concern Score: 0.37
0.40
0.30
0.20
0.10
Max Concerns Flow Count Spike: 0.00
Max Concerns Flow Fwd: 0.73
0.80
0.60
0.40
0.20
Max Concerns Bmp Withdraw: 0.19
0.20
0.15
0.10
0.05
Max Concerns Bmp Update: 0.00
Max Concerns Oc Interface State: 0.00
Max Concerns Traffic Drop: 0.00
Max Concerns Bmp Peer Down: 0.00
40
22:45
22:50
22:55
23:00
23:05
23:10
23:15
23:20
23:25
23:30
23:35
23:40
23:45
23:50
23:55

Cosmos Bright Lights Anomaly Detection – 64497:4965

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 been observed on Inter-AS option B ASBRs and route-reflectors.

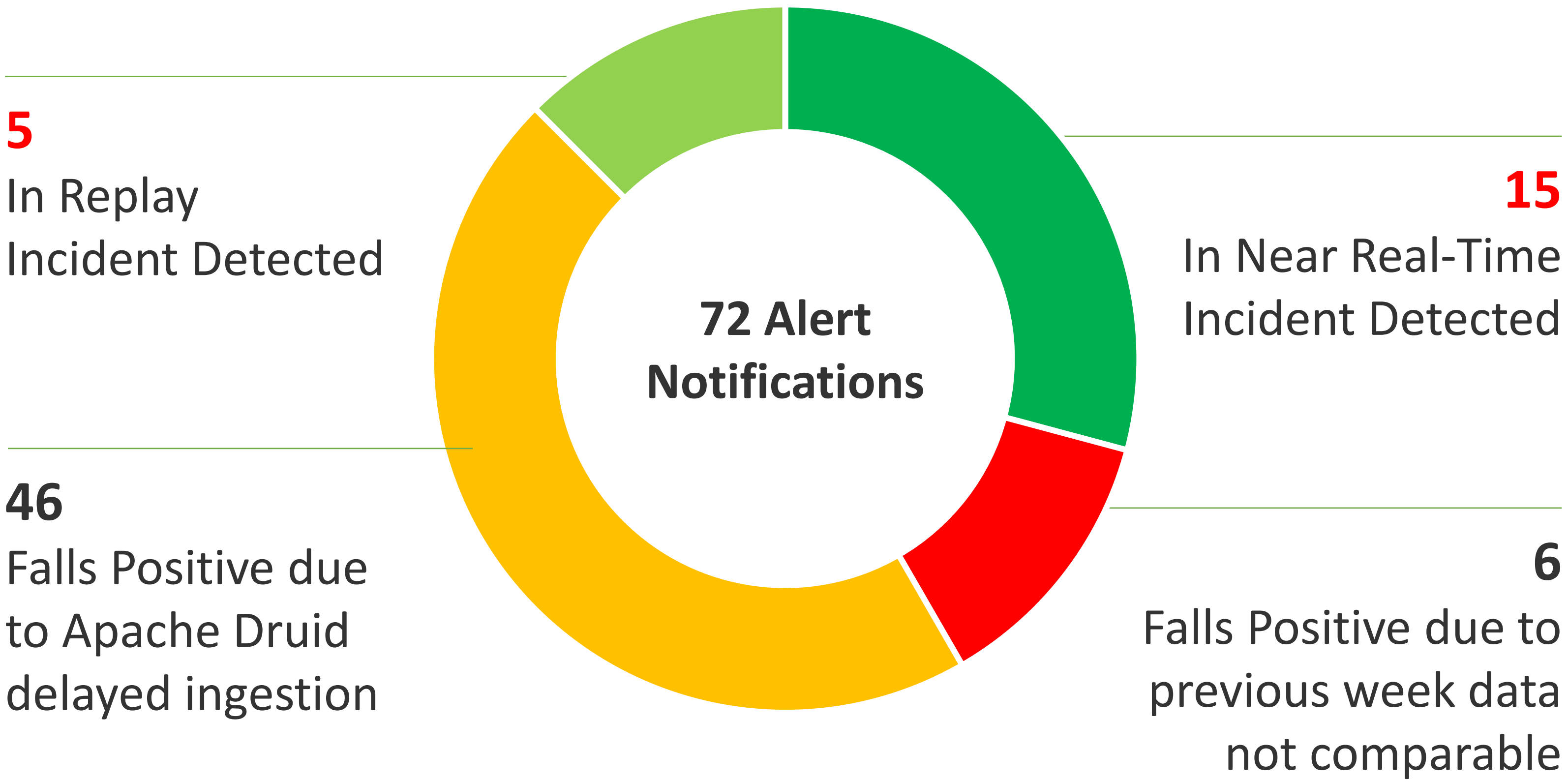
With draft-ietf-grow-bmp-path-marking-tlv path status changed could have been observed on Inter-AS option B ASBRs.

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

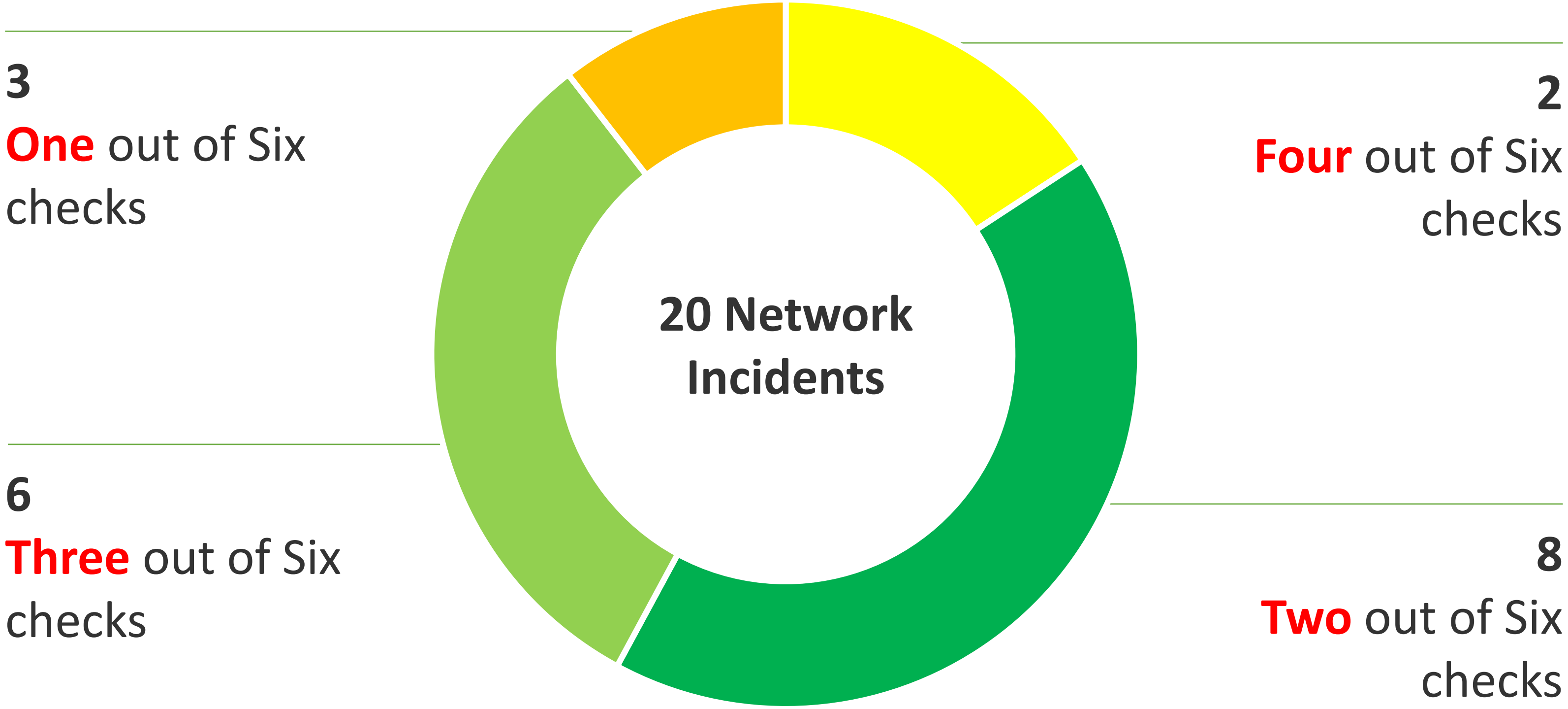


Key Facts in V0 (2023-2024)

- 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



20 Network Incidents

3
One out of Six checks

6
Three out of Six checks

2
Four out of Six checks

8
Two out of Six checks

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.