# Swisscom: Network Incident Network Analytics Postmortem

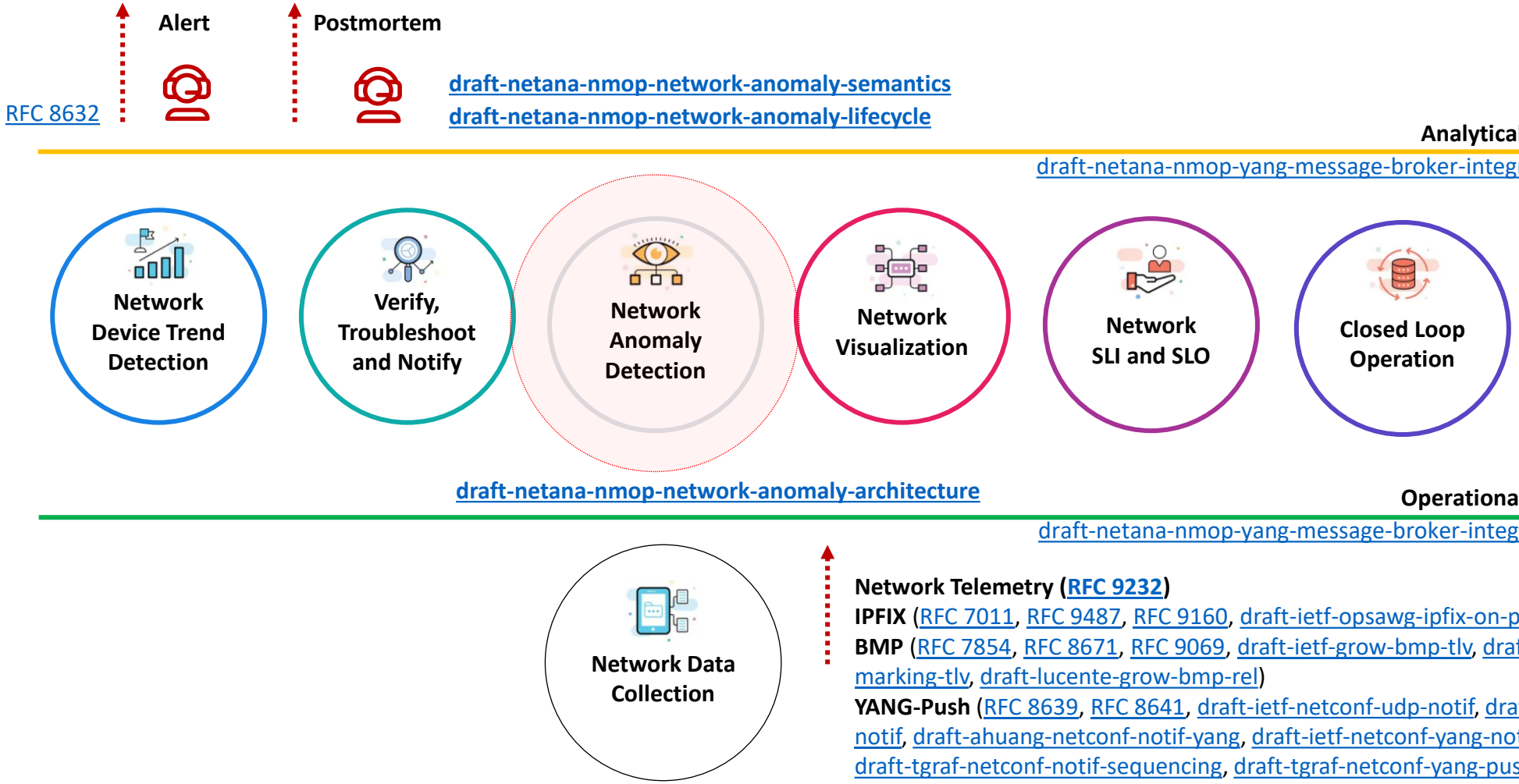
Describes an incident in terms of
what happened,
which operational metrics where available,
which analytical metrics described the symptoms and
what improvements in the network anomaly detection system and network telemetry protocols are proposed.

thomas.graf@swisscom.com

06. September 2024

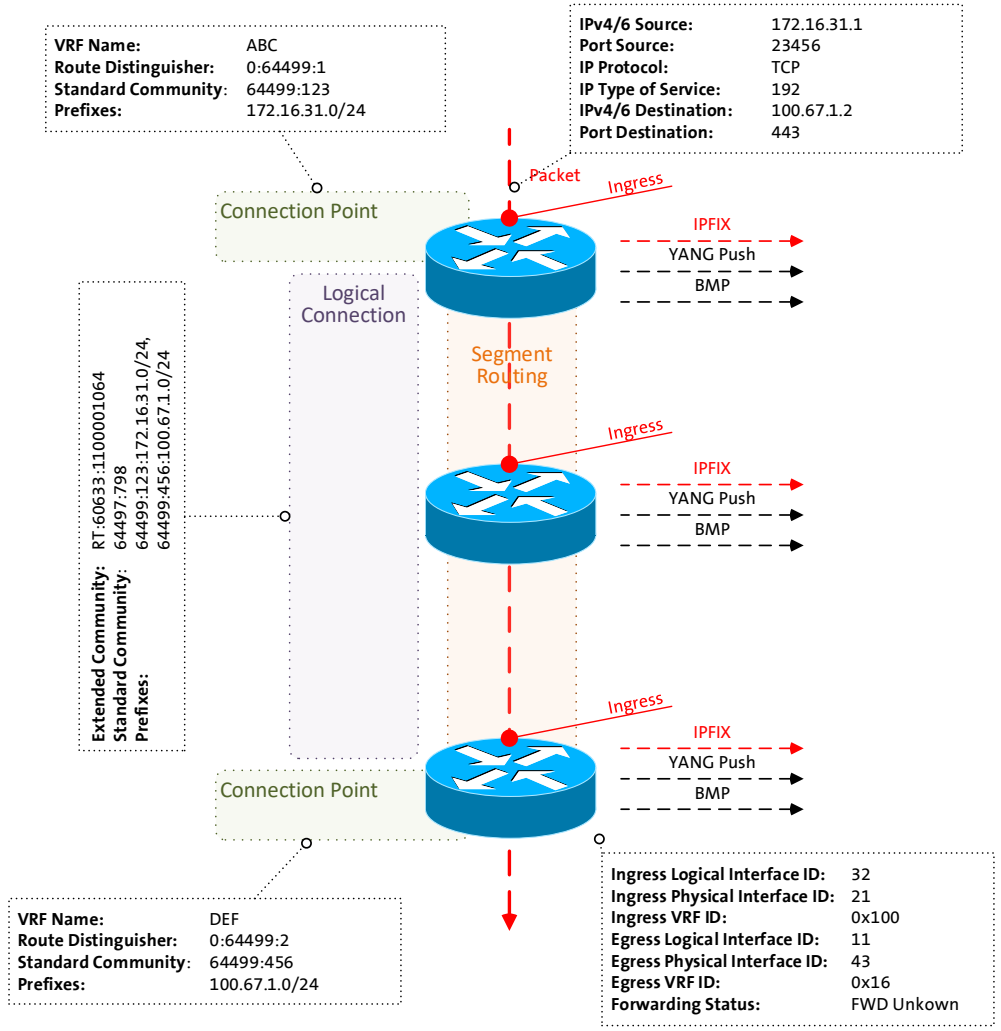
# Data Mesh organizes Data in Organizations

## Enables Network Analytics use cases



# 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.

# August 14th, SRv6 IS-IS ABR Route Aggregation

## Post Maintenance Window Analysis


**Cosmos Bright Lights Anomaly Detection Results for 15 L3 VPN's Traversing SRv6 Core**

**Maintenance Window started on August 14th 00:04 and ended at 01:12. In total 15 configuration steps were performed.** These configuration steps involved: IS-IS overload-bit on ABR, ABR IS-IS L1/2 to L2/L2 and PE L1 to L2 migration, IS-IS locator summarization.

**Throughout the maintenance window,** in overlay topology changes, traffic volume and flow count changes, forwarding plane drops and customer data plane TCP congestion were measured and observed but nor alerted. **In SRv6 underlay, forwarding plane drops were measured and observed but not alerted.**

Network operation center **was alerted** that 10 VOIP service calls were dropped, mobile subscriber control plane was interrupted. Both platform teams were notified **but did not gain insights in causality.**

**At 01:51,** the maintenance window implementers informed network operation center that all configuration changes were performed, and no connectivity service impact was observed.

**At 10:22,** network operation center was being asked wherever connectivity service impact was visible and reasoning behind.

**At 11:12,** network operation center confirmed that wherever connectivity service impact is visible and most likely being related with performed maintenance window.

**During Post Maintenance Window Analysis,** connectivity service impact on 3 previous maintenance windows, August 6th, August 7th and August 13th were discovered.

# August 14th, SRv6 IS-IS ABR Route Aggregation

## Network Telemetry Coverage

IPFIX configured on P and PE SRv6 nodes on SRv6 and IPv4/6 VRF unicast enabled interfaces. Capturing L3 IPv4/6 and L2 Ethernet overlay customer data plane **and underlay SRv6 provider data plane metrics on SRv6 enabled interfaces,** and IPv4/6 and L2 Ethernet overlay customer data plane metrics on IPv4/6 VRF unicast enabled interfaces.

**-> Shape, means that we are engaged in IETF standardization, vendor implementations and running code. IPv4/6 unicast customer data plane visibility is in vital, SRv6 data plane visibility is in applied, On-Path delay is in operational stage.**

BMP Adj-RIB In post-policy on BGP VPNv4 /6 and IPv4/6 VRF unicast peers and Local-RIB on all RIB's configured on SRv6 PE's. BMP Adj-RIB In post-policy on BGP VPNv4 /6 peers on Route Reflectors configured.

**-> Shape, means that we are engaged in IETF standardization, vendor implementations and running code. BMP Local RIB data plane visibility is in applied, BMP Path Marking is in operational stage.**

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

**-> Take, means that current YANG-Push legacy implementation is used without any vendor code change and is in accepted stage. However, IETF YANG-Push is shape and is in operational state.**

# August 6/7th, SRv6 IS-IS ABR Route Aggregation

## Post Maintenance Window Analysis


**Cosmos Bright Lights Anomaly Detection Results for 15 L3 VPN's Traversing SRv6 Core at Location AAR**


**Cosmos Bright Lights Anomaly Detection Results for 15 L3 VPN's Traversing SRv6 Core at Location OLT**

# August 13/14th, SRv6 IS-IS ABR Route Aggregation

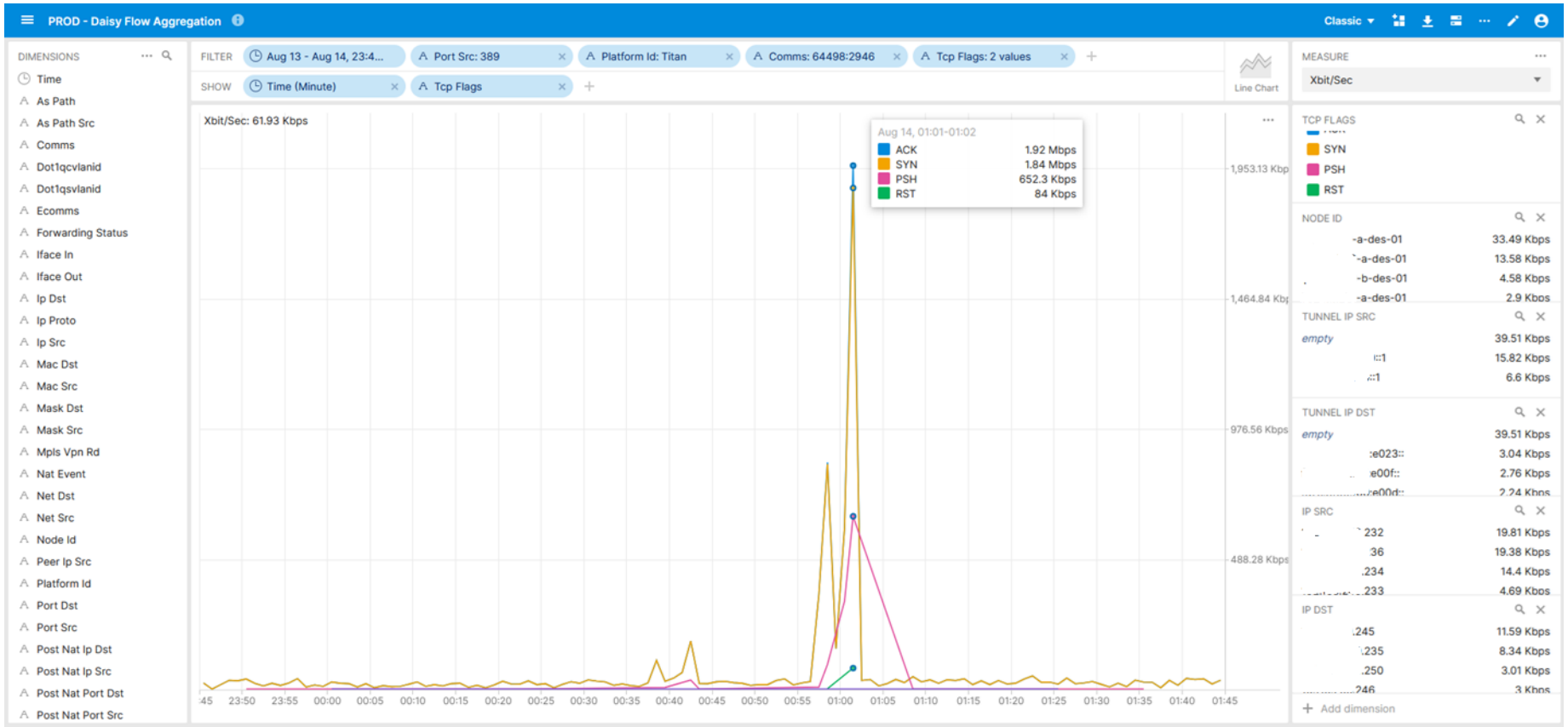
## Post Maintenance Window Analysis


**Cosmos Bright Lights Anomaly Detection Results for 15 L3 VPN's Traversing SRv6 Core at Location ZHB**

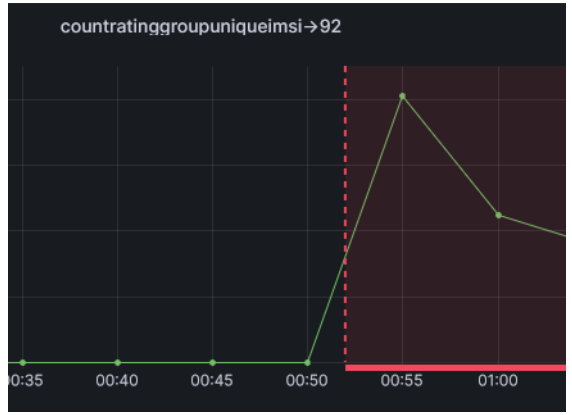

**Cosmos Bright Lights Anomaly Detection Results for 15 L3 VPN's Traversing SRv6 Core at Location ZHH**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## Mobile Subscriber Management Control Plane




**SRv6 forwarding plane and customer data plane.** Shows on a particular L3 VPN the amount of TCP SYN and RST **from L4 port 389 were originated** and **through which PE nodes and with which SRv6 SID's** the traffic was forwarded with.
**Remark: IE6 tcpControlBits is a none key field.**

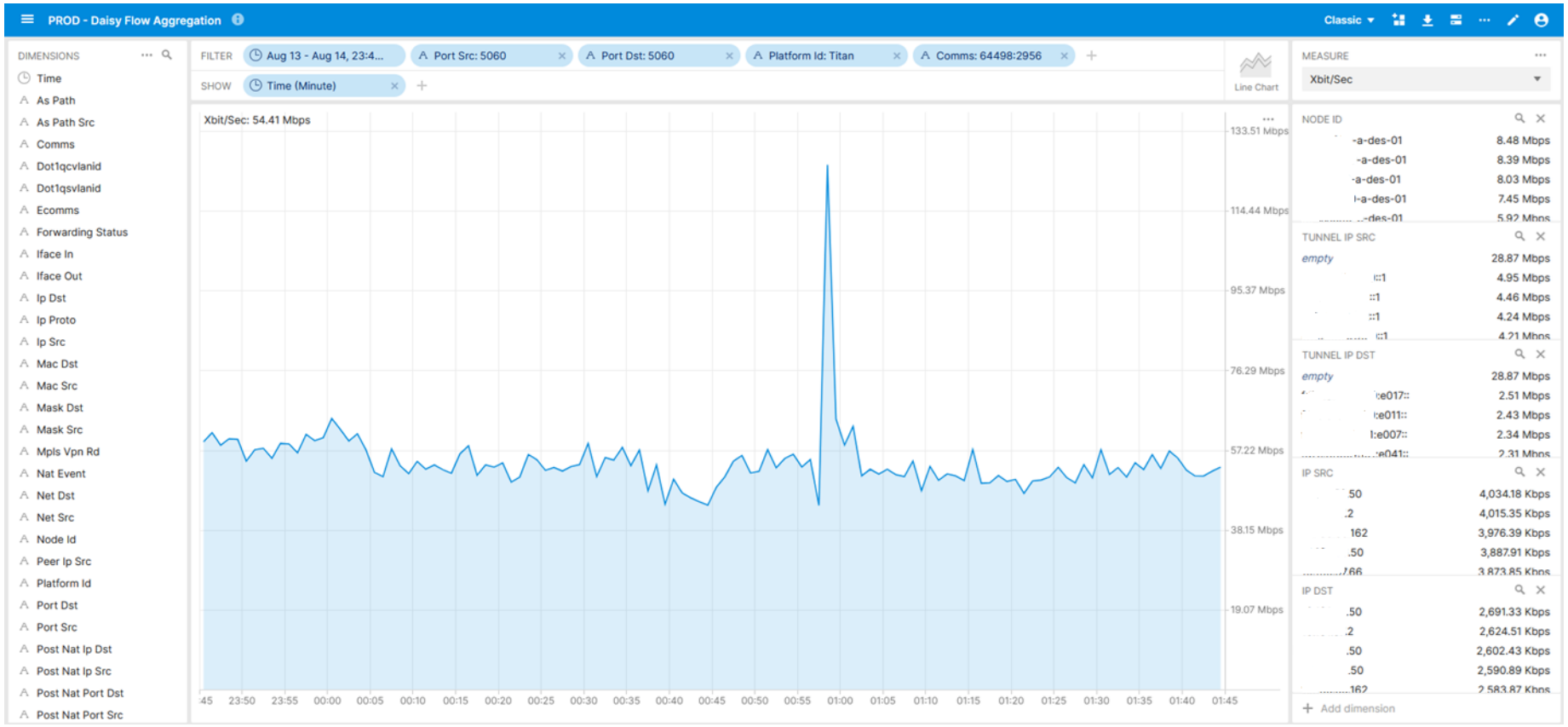



**Resulted in Mobile Fallback Subscriber Session Count**

**Mobile Subscriber Management Control Plane Overlay Congestion**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## Mobile Subscriber Management Control Plane

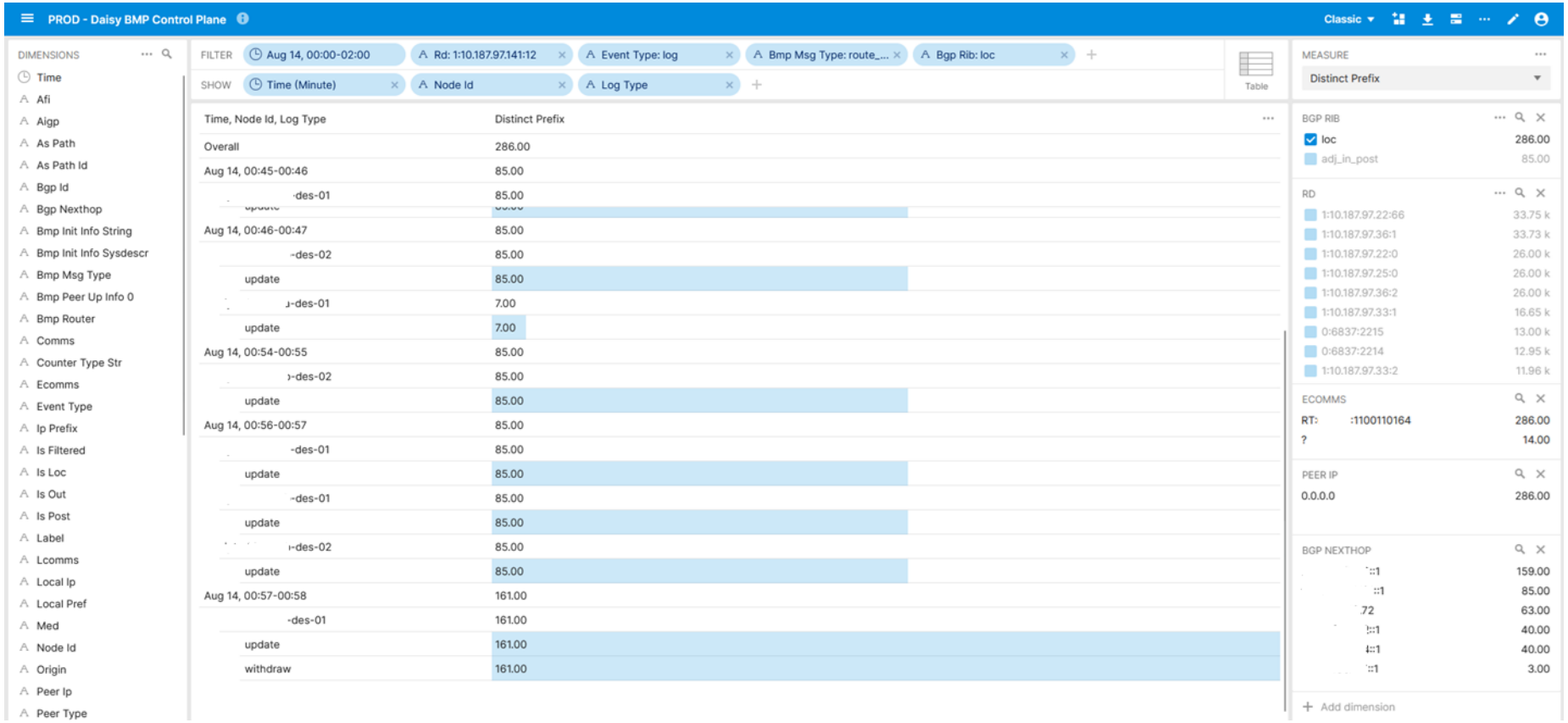



**SRv6 forwarding plane and customer data plane.** Shows on a particular L3 VPN the amount of traffic **between L4 port 5060** and **through which PE nodes and with which SRv6 SID's** the traffic was forwarded with.

**VOIP SIP Signaling Overlay Congestion**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## L3 VPN Overlay Topology Change

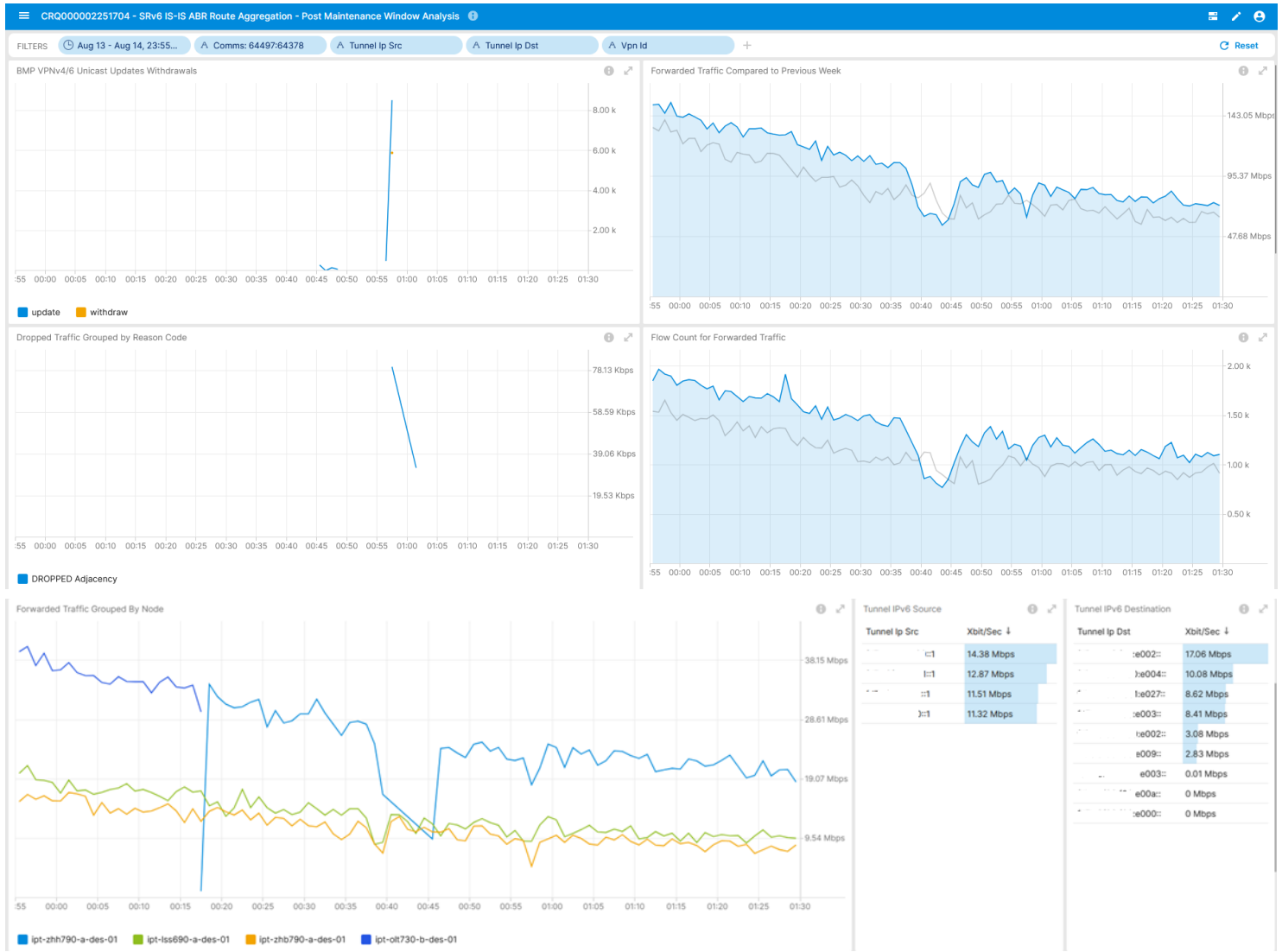



BMP BGP Local-RIB **L3 VPN topology change for a particular BGP route-distinguisher**. **Only best path is exported due to implementation limitation.** Shows in time frame 00:57-58 that **prefixes were removed from the VRF routing table on a particular PE node**. Leading to potential blackholing.

**BGP Overlay VRF Endpoint Topology Change**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## 64497:64378 SRv6 L3 VPN – Operational Network Telemetry Metrics




**Logical Connection 64497:64378 SRv6 L3 VPN Overlay Operational Metrics**

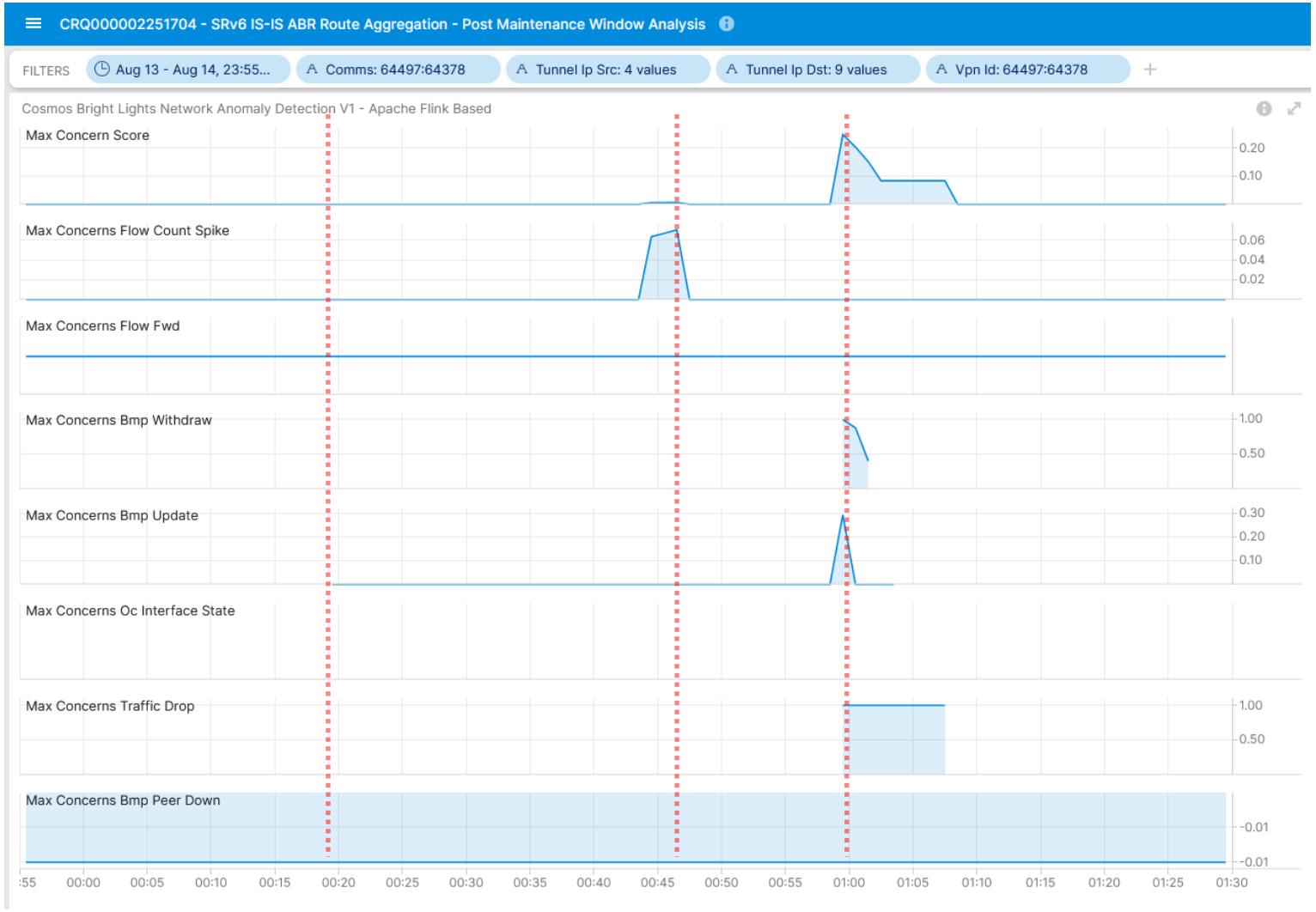
**Logical Connection 64497:64378 SRv6 L3 VPN Overlay and Underlay Operational Metrics**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## 64497:64378 SRv6 L3 VPN – Anomaly Detection - Live

**Concern Score: 0.25**
Flow Count Spike: **0.07**
Missing Traffic: **0.22**
Traffic Drop: **1.00**
BMP Update/Withdrawal: **0.29/ 1.00**

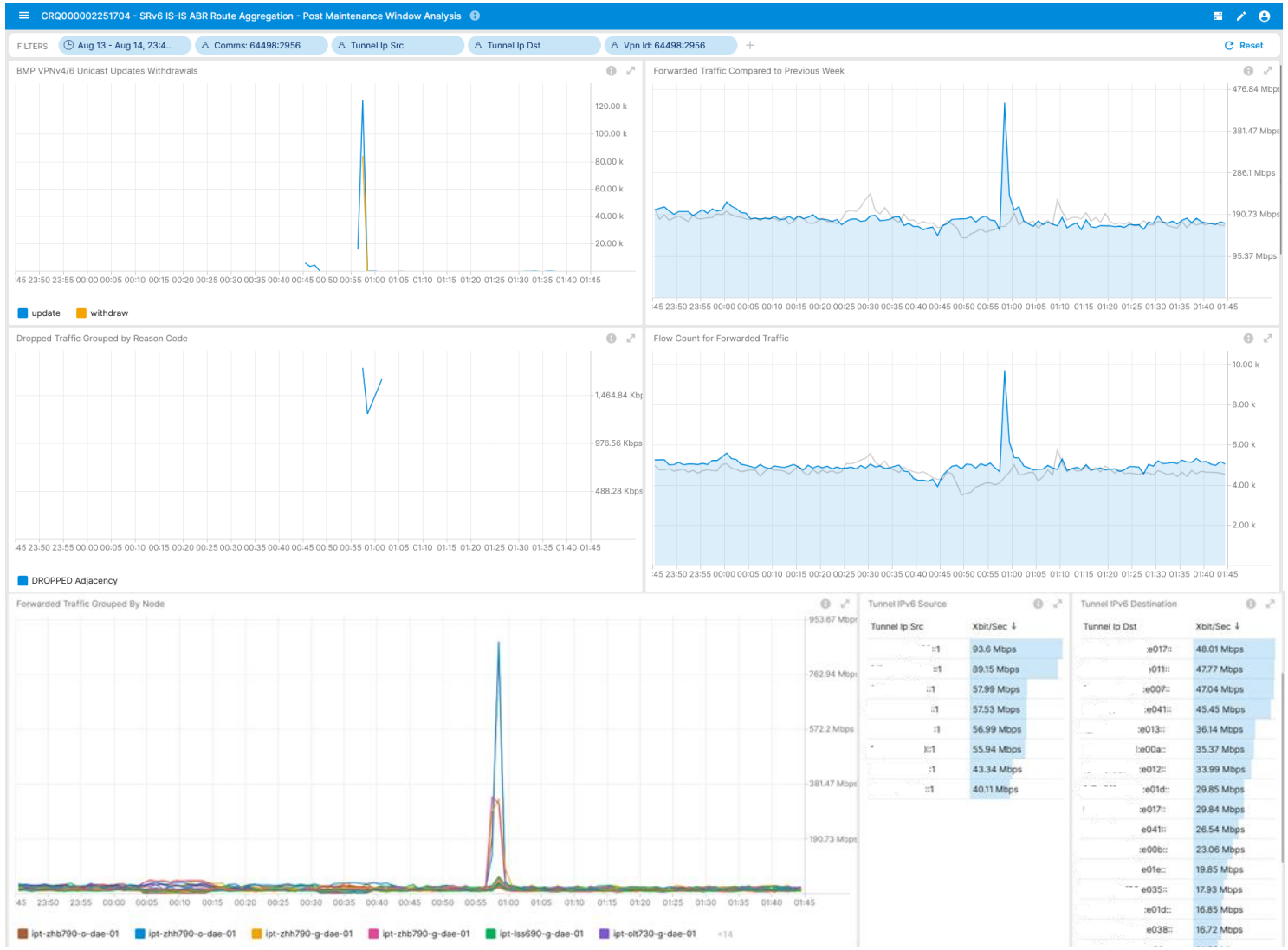
*Real-Time Streaming under Development*




- **BMP route-monitoring Update/Withdraw check recognized topology change.**
- BMP peer Down/Up check did not apply.
- Interface Down/Up check did not apply.
- **Traffic Drop spike check recognized traffic drop due to topology change.**
- **Missing Traffic check recognized traffic loss.**
- **Increased or decreased Flow Count check recognized congestion.**
- **Overall: 4 out of 6 checks have detected the BGP topology change. Real-time streaming implementation exceeds expectations.**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## 64497:2956 SRv6 L3 VPN – Operational Network Telemetry Metrics

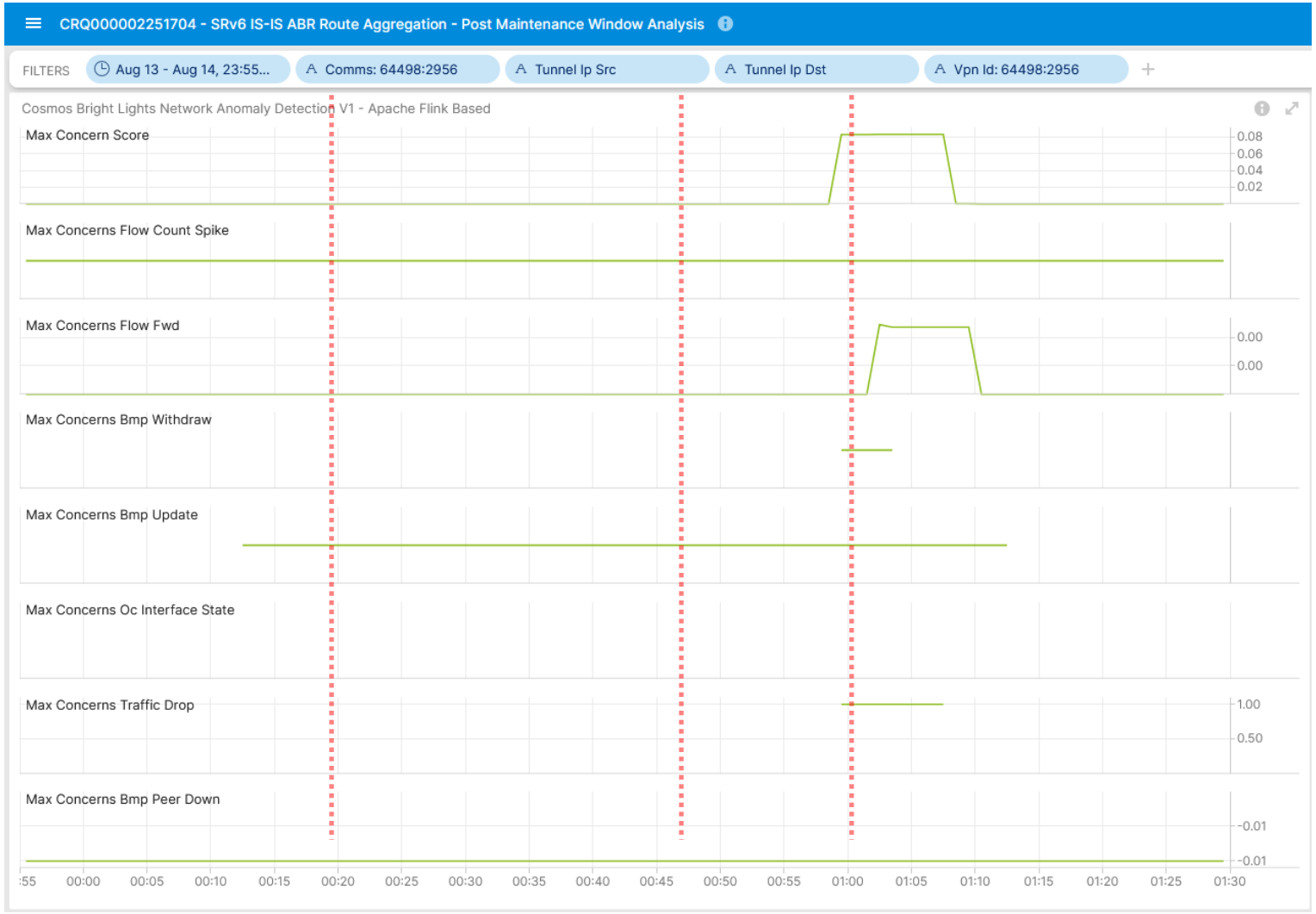



**Logical Connection 64498:2956 SRv6 L3 VPN Overlay Operational Metrics**

**Logical Connection 64498:2956 SRv6 L3 VPN Overlay and Underlay Operational Metrics**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## 64497:2956 SRv6 L3 VPN – Anomaly Detection - Live




**Concern Score: 0.08**
Flow Count Spike: **0.00**
Missing Traffic: **0.00**
Traffic Drop: **1.00**
BMP Update/Withdrawal: **0.00/ 0.00**

*Real-Time Streaming under Development*

**BMP route-monitoring Update/Withdraw check did not recognize topology change.**

— BMP peer Down/Up check did not apply.

— Interface Down/Up check did not apply.

**Traffic Drop spike check recognized traffic drop due to topology change.**

— **Missing Traffic check did not apply.**

**Increased or decreased Flow Count check did not recognized congestion.**

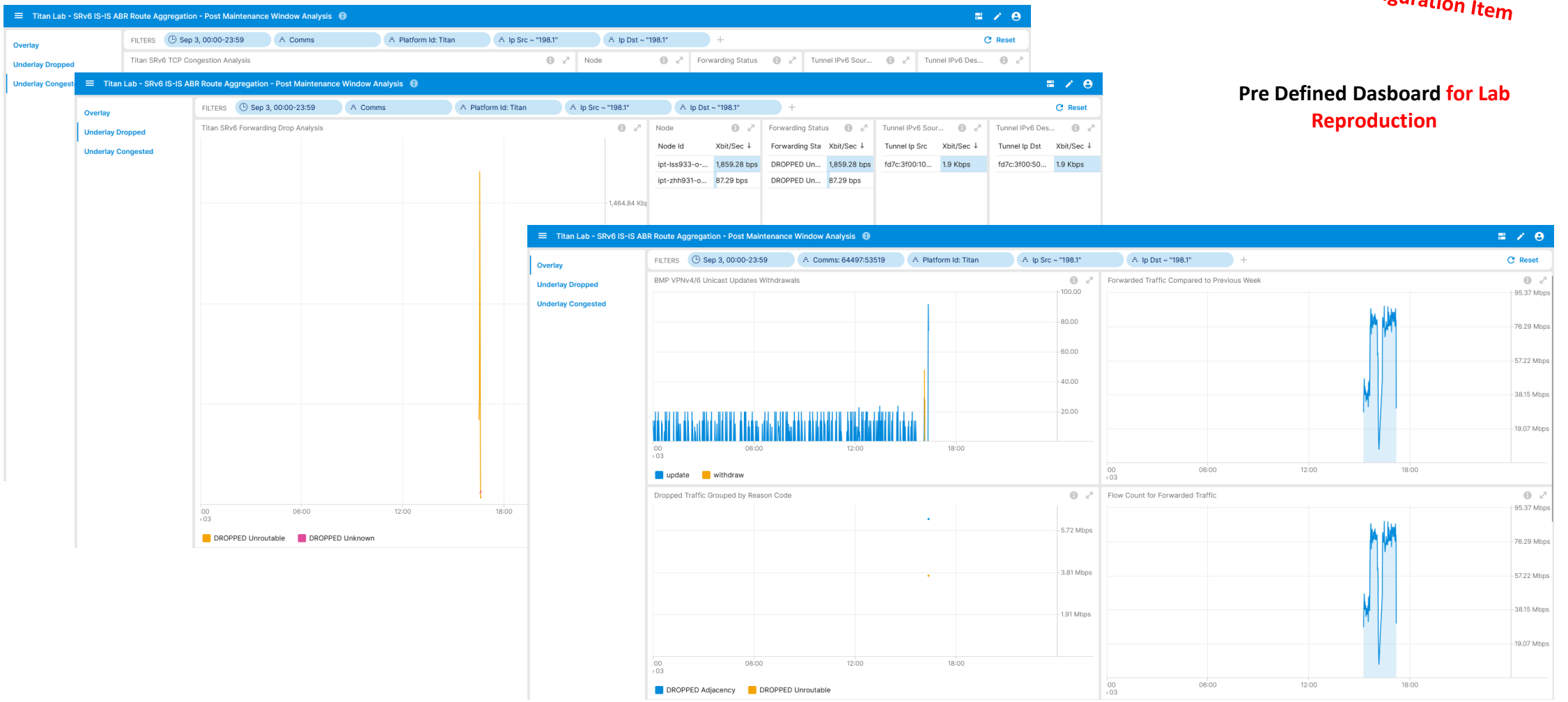
**Overall: 1 out of 6 checks have detected the BGP topology change. Real-time streaming implementation.**
**Auto profiling under implementation.**

# August 14th, SRv6 IS-IS ABR Route Aggregation

## Lab Repro In Progress

**Reproduction Partial**
**Successful**
**Identified Root Cause and Configuration Item**

**Pre Defined Dasboard for Lab Reproduction**



# What to do next?

- Establish a network topology and Network Telemetry lab reproduction and verify configuration change with collected operational metrics.
  **-> Showing first results**
- SRv6 Mobile Connectivity NRE REP-8 Preparation and Execution
  **-> Has started**

## What went well?

Work in progress Cosmos Bright Lights real-time streaming Anomaly Detection exceeded in 2 out of 6 cases our expectations, **matching 100% our intend. Alert notifications were sent 120-180 seconds after operational metrics in the network were observed.** 60 seconds variable delay is due to 2 step flow aggregation process. The other 4 cases would have also worked perfectly if auto profiling feature would have been implemented already.

Based on experience in Seamless MPLS-SR migration, indirect visibility on provider edge is not sufficient to monitor core. We derived the necessity to monitor underlay, however had to compromise in SRv6 limiting to forwarding plane only, which works exceptionally well, and unfortunately not monitoring IS-IS control plane on day 1 since innovation curve was to high compared to resources available.

Anycast fast failover from ZHH to OLT with pre cached BMP collected BGP routing table avoided that undesired underlay routing topology change had negative impact on the Network Telemetry data collection.

Same dashboard with different data cubes **helped to reproduce the issue in the lab more easily and identified a configuration error in the IS-IS redistribution.**

## What could be improved?

Partially missing profiling (work in progress) for flow aggregation leads in certain L3 VPN's into false positive. Consider profiling for BMP update/withdrawals as well.

IS-IS control plane visibility is missing. This would have helped to understand the routing topology state change. Cisco IOS XR does not support BGP-LS in BMP Local-RIB. At IETF, two proposals, draft-raszuk-lsr-imp and draft-gu-opsawg-network-monitoring-igp have been proposed to export IGP LSDB directly without redistributing to BGP-LS, which for SRv6 is very desirable due to SRv6 feature dependency on BGP-LS.

Forwarding plane path visibility (Passive Hybrid Type 1) is missing. This would have helped to understand the exact forwarding path for each packet.

With SRv6 next-hop attribute (SRv6 Endpoint Behaviors) in data collection decoded, change of VPNv4/6 unicast path would have been visible. Consider to remove or reduce 1min time bucketing in TSDB.

Taken connectivity service, the network relationship, not into account, **none of the involved connectivity service incident parties were able to understand that their activity is related to each other.**

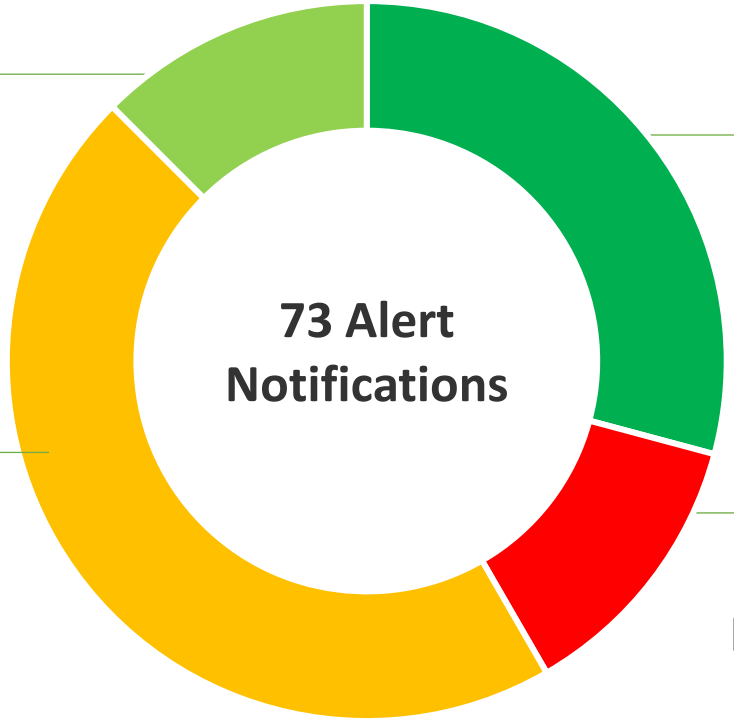
Observing configuration state change with Transaction ID (draft-ietf-netconf-transaction-id , draft-ietf-netconf-configuration-tracing) would have helped to understand which config change contributed to which topology change.

# Swisscom - Cosmos Bright Lights PoC Summary

## After 21 Incidents and 18 Months Time

**5**
In Replay
Incident Detected

**46**
Falls Positive due to Apache Druid delayed ingestion




**16**
In Near Real-Time
Incident Detected

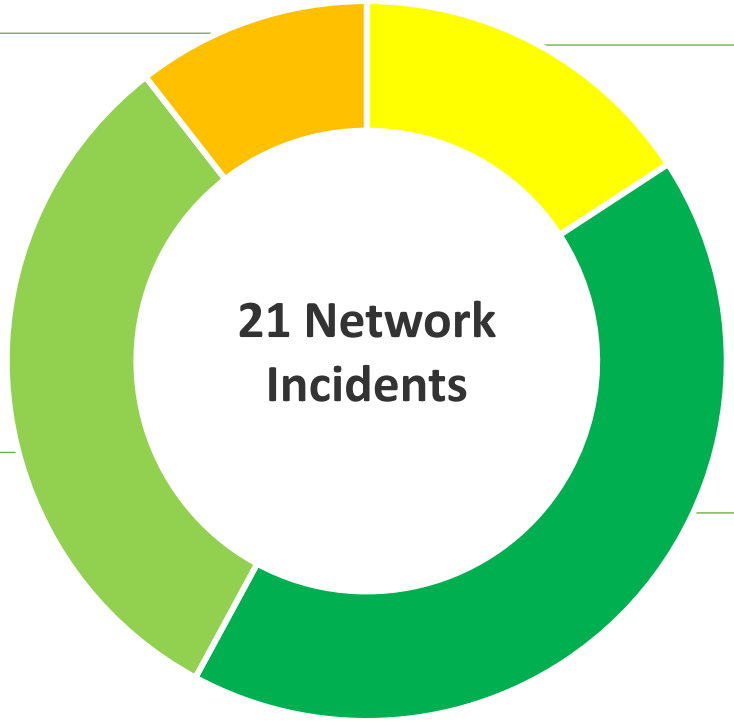
**6**
Falls Positive due to previous week data not comparable

**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




**3**
**One** out of Six checks

**4**
**Four** out of Six checks

**6**
**Three** 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.