# Swisscom: SRv6 Network Incident Network Analytics Postmortem

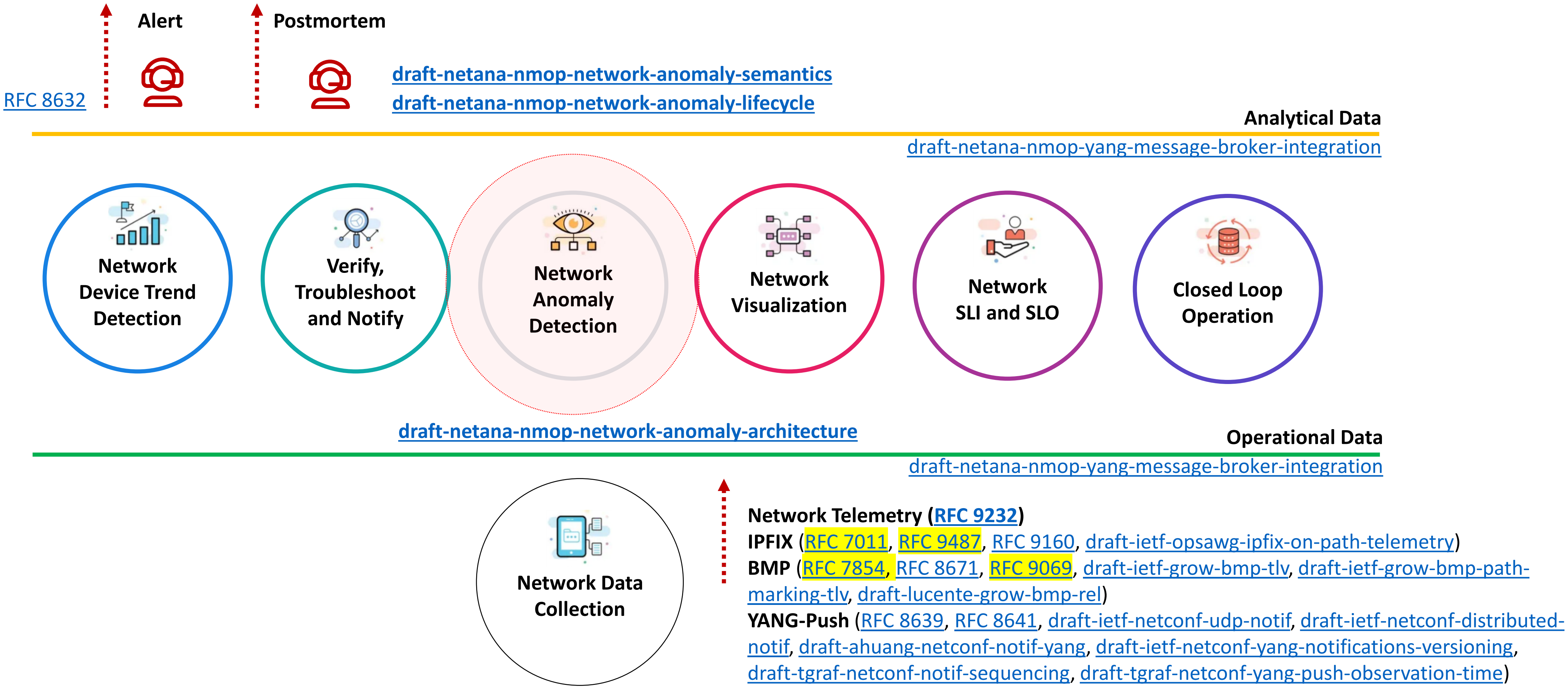
Describes an incident in terms of
what happened,
which operational metrics where available,
which analytical metrics described the symptoms and
what improvements in the network anomaly detection
system and network telemetry protocols are proposed.

thomas.graf@swisscom.com

27. October 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**

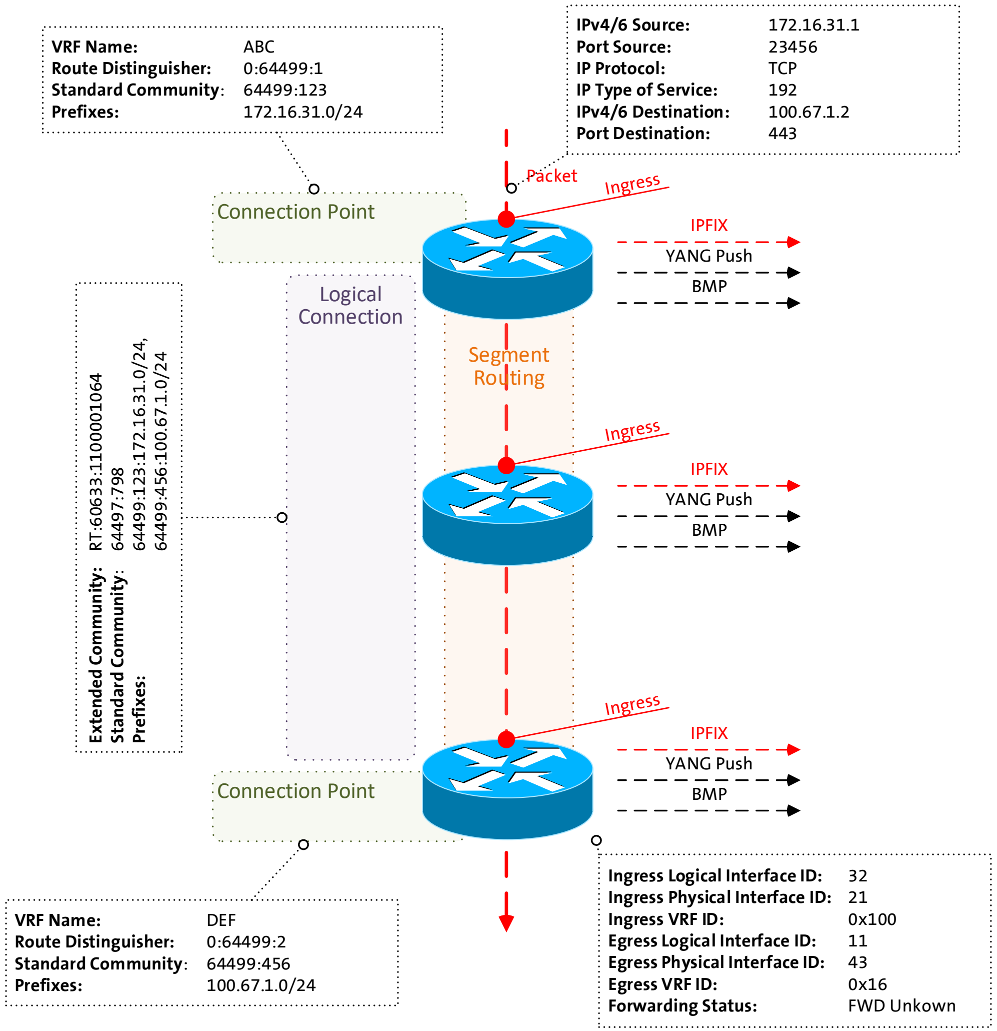
draft-netana-nmop-yang-message-broker-integration

**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)

# 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,<br>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.

# Problem Statement and Motivation

## How it is being addressed in which document

## Network Anomaly Detection

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

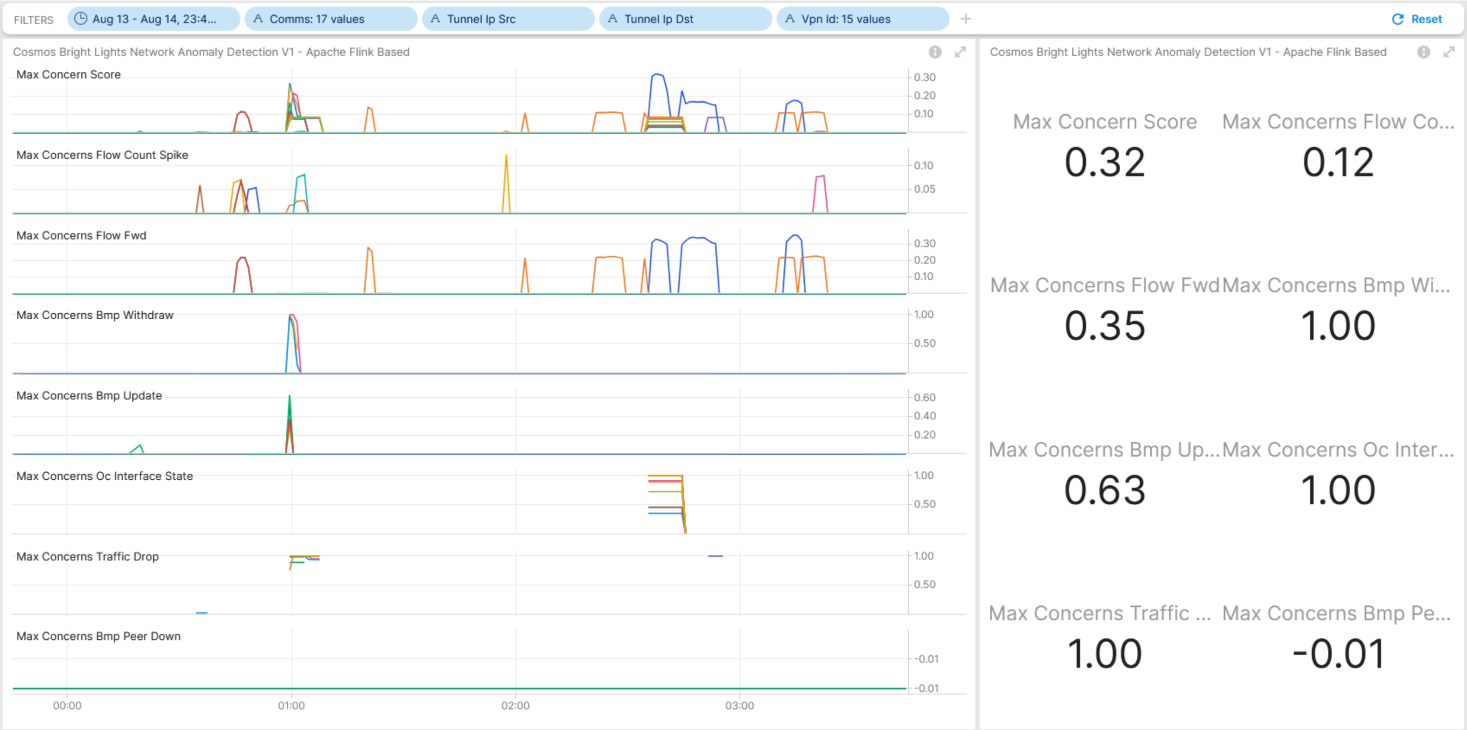
In order to achieve this objective, automation in network monitoring is required. This automation needs to monitor network changes holistically by monitoring all 3 network planes simultaneously and detect whether that change is service disruptive.

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.

- draft-ietf-nmop-network-anomaly-architecture describes the motivation and architecture and the relationship to other two documents.
- draft-netana-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-netana-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.

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

## Post Maintenance Window Analysis



FILTERS: Aug 13 - Aug 14, 23:4... | Comms: 17 values | Tunnel Ip Src | Tunnel Ip Dst | Vpn Id: 15 values | Reset

Cosmos Bright Lights Network Anomaly Detection V1 - Apache Flink Based

Cosmos Bright Lights Network Anomaly Detection V1 - Apache Flink Based

Max Concern Score 0.32

Max Concerns Flow Co... 0.12

Max Concerns Flow Fwd 0.35

Max Concerns Bmp Wi... 1.00

Max Concerns Bmp Up... 0.63

Max Concerns Oc Inter... 1.00

Max Concerns Traffic ... 1.00

Max Concerns Bmp Pe... -0.01

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

**Maintenance Window with 15 configuration steps started on August 14th 00:04 and ended at 01:12.** 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**. 10 VOIP service calls were dropped, and mobile subscriber control plane was interrupted. Both platform teams were notified **but did not find 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 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.

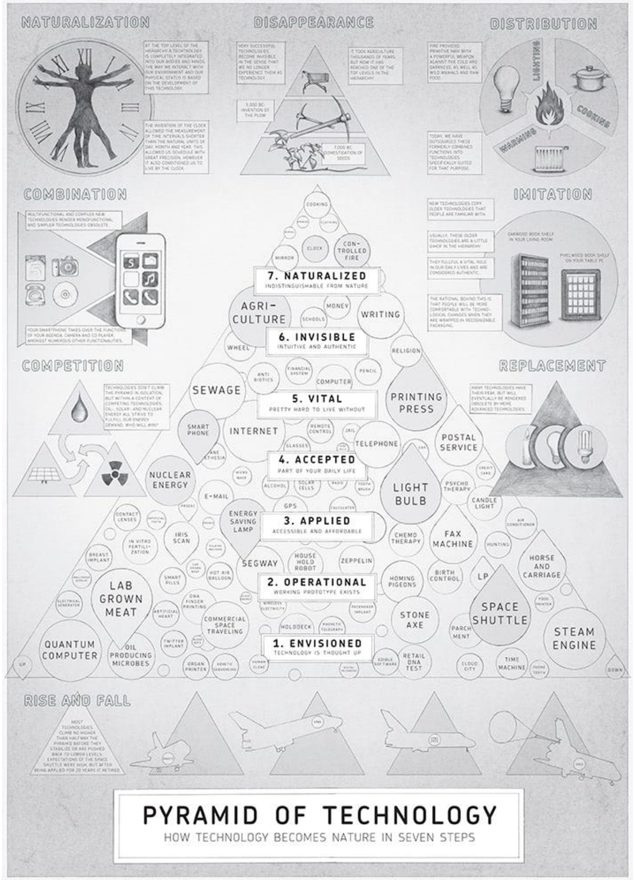
**-> Shape, means that we are engaged in IETF standardization, vendor implementations and running code. IPv4/6 unicast customer data plane visibility is in vital, SRv6 data plane visibility is in applied, On-Path delay is in operational stage.**

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.**

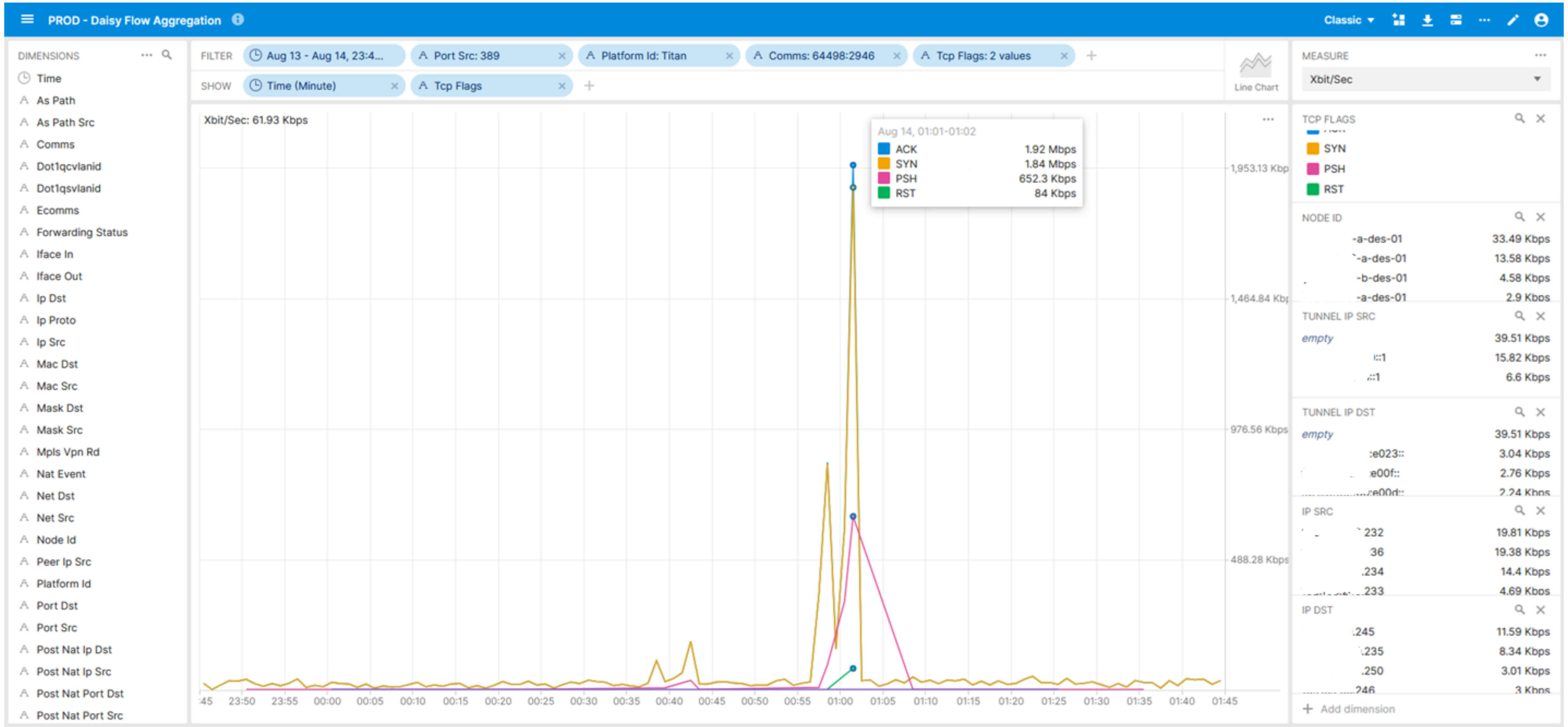
YANG Push Legacy on most nodes enabled but not relevant for this use case.

**-> 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 14th, SRv6 IS-IS ABR Route Aggregation

## Mobile Subscriber Management Control Plane



FILTER: Aug 13 - Aug 14, 23:4... | Port Src: 389 | Platform Id: Titan | Comms: 64498:2946 | Tcp Flags: 2 values

SHOW: Time (Minute) | Tcp Flags

MEASURE: Xbit/Sec

Xbit/Sec: 61.93 Kbps

Aug 14, 01:01-01:02

| | |
|---|---|
| 🟦 ACK | 1.92 Mbps |
| 🟧 SYN | 1.84 Mbps |
| 🟪 PSH | 652.3 Kbps |
| 🟩 RST | 84 Kbps |

NODE ID

| | |
|---|---|
| -a-des-01 | 33.49 Kbps |
| -a-des-01 | 13.58 Kbps |
| -b-des-01 | 4.58 Kbps |
| -a-des-01 | 2.9 Kbps |

TUNNEL IP SRC

| | |
|---|---|
| *empty* | 39.51 Kbps |
| ::1 | 15.82 Kbps |
| ::1 | 6.6 Kbps |

TUNNEL IP DST

| | |
|---|---|
| *empty* | 39.51 Kbps |
| :e023:: | 3.04 Kbps |
| :e00f:: | 2.76 Kbps |
| :e00d:: | 2.24 Kbps |

IP SRC

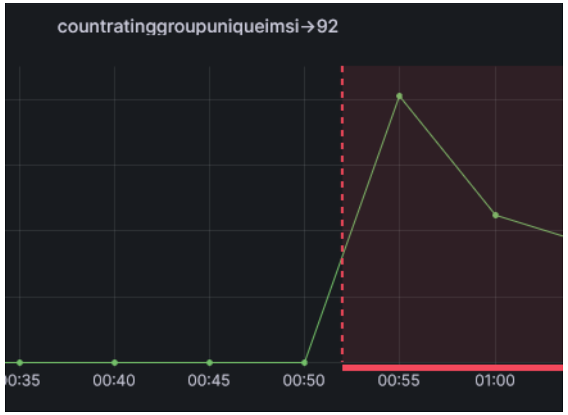
| | |
|---|---|
| 232 | 19.81 Kbps |
| 36 | 19.38 Kbps |
| .234 | 14.4 Kbps |
| .233 | 4.69 Kbps |

IP DST

| | |
|---|---|
| .245 | 11.59 Kbps |
| .235 | 8.34 Kbps |
| .250 | 3.01 Kbps |
| .246 | 3 Kbps |

**Mobile Subscriber Management Control Plane Overlay Congestion**

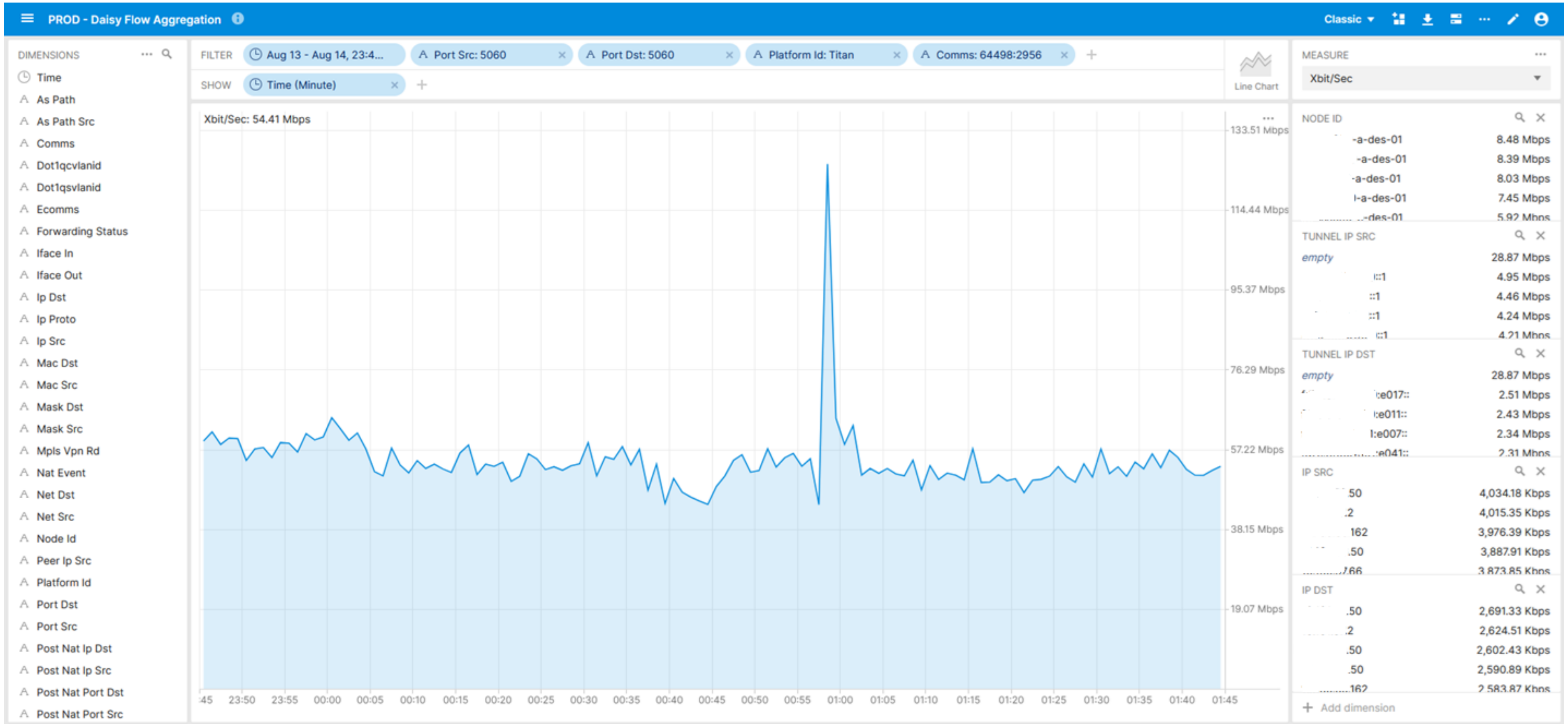
**SRv6 forwarding plane and customer data plane.** Shows on a particular L3 VPN the amount of TCP SYN and RST **from L4 port 389 were originated** and **through which PE nodes and with which SRv6 SID's** the traffic was forwarded with. **Remark: IE6 tcpControlBits is a none key field.**



**Resulted in Mobile Fallback Subscriber Session Count**

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

## Mobile Subscriber Management Control Plane



FILTER: Aug 13 - Aug 14, 23:4... | Port Src: 5060 | Port Dst: 5060 | Platform Id: Titan | Comms: 64498:2956

SHOW: Time (Minute)

Xbit/Sec: 54.41 Mbps

MEASURE: Xbit/Sec

| NODE ID | |
|---|---|
| -a-des-01 | 8.48 Mbps |
| -a-des-01 | 8.39 Mbps |
| -a-des-01 | 8.03 Mbps |
| -a-des-01 | 7.45 Mbps |
| -des-01 | 5.92 Mbps |

| TUNNEL IP SRC | |
|---|---|
| *empty* | 28.87 Mbps |
| ::1 | 4.95 Mbps |
| ::1 | 4.46 Mbps |
| ::1 | 4.24 Mbps |
| ::1 | 4.21 Mbps |

| TUNNEL IP DST | |
|---|---|
| *empty* | 28.87 Mbps |
| :e017:: | 2.51 Mbps |
| :e011:: | 2.43 Mbps |
| :e007:: | 2.34 Mbps |
| :e041:: | 2.31 Mbps |

| IP SRC | |
|---|---|
| .50 | 4,034.18 Kbps |
| .2 | 4,015.35 Kbps |
| 162 | 3,976.39 Kbps |
| .50 | 3,887.91 Kbps |
| 766 | 3,873.85 Kbps |

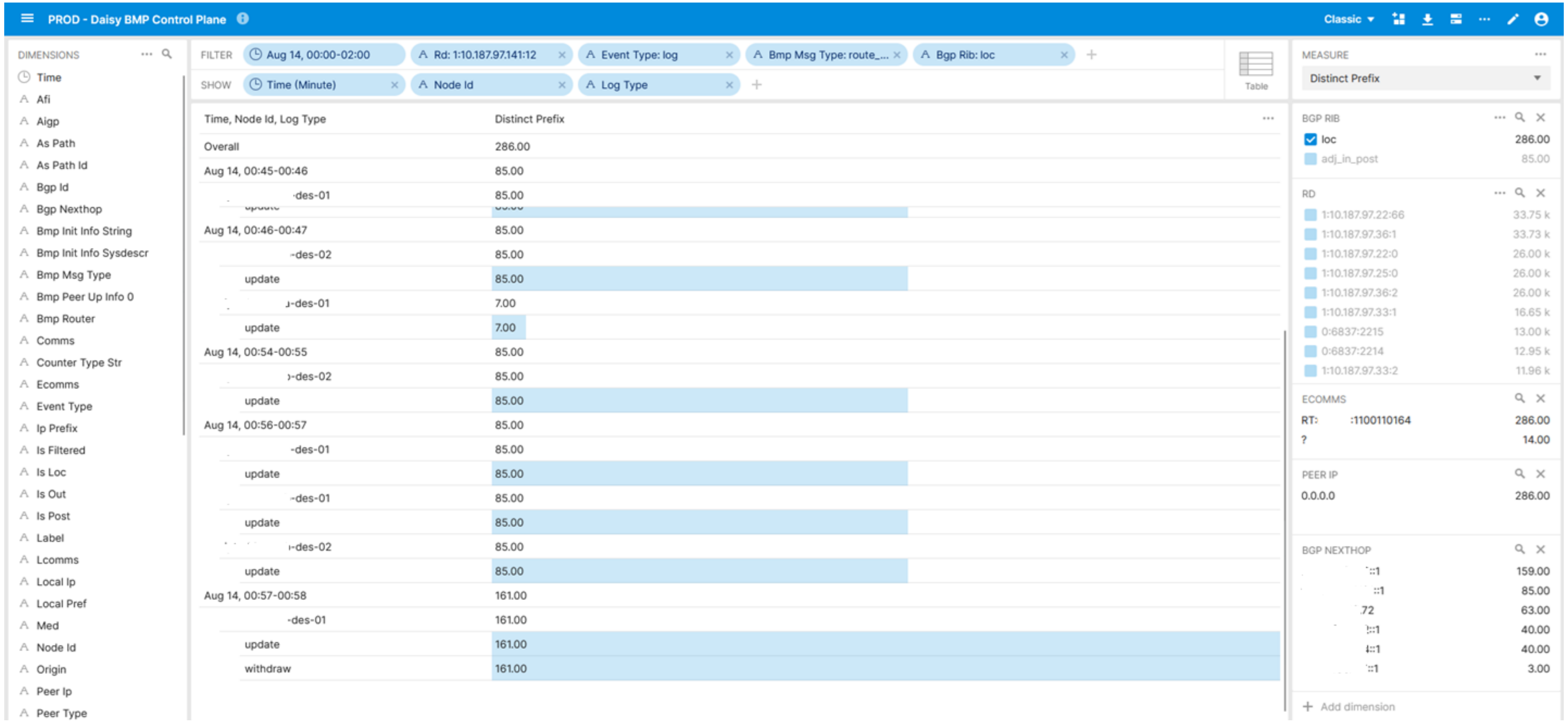
| IP DST | |
|---|---|
| .50 | 2,691.33 Kbps |
| .2 | 2,624.51 Kbps |
| .50 | 2,602.43 Kbps |
| .50 | 2,590.89 Kbps |
| .162 | 2,583.87 Kbps |

**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



PROD - Daisy BMP Control Plane

Classic ▾

DIMENSIONS

- Time
- Afi
- Aigp
- As Path
- As Path Id
- Bgp Id
- Bgp Nexthop
- Bmp Init Info String
- Bmp Init Info Sysdescr
- Bmp Msg Type
- Bmp Peer Up Info 0
- Bmp Router
- Comms
- Counter Type Str
- Ecomms
- Event Type
- Ip Prefix
- Is Filtered
- Is Loc
- Is Out
- Is Post
- Label
- Lcomms
- Local Ip
- Local Pref
- Med
- Node Id
- Origin
- Peer Ip
- Peer Type

FILTER: Aug 14, 00:00-02:00 × | Rd: 1:10.187.97.141:12 × | Event Type: log × | Bmp Msg Type: route_... × | Bgp Rib: loc × | +

SHOW: Time (Minute) × | Node Id × | Log Type × | +

Table

| Time, Node Id, Log Type | Distinct Prefix |
|---|---|
| Overall | 286.00 |
| Aug 14, 00:45-00:46 | 85.00 |
| -des-01 | 85.00 |
| update | 85.00 |
| Aug 14, 00:46-00:47 | 85.00 |
| -des-02 | 85.00 |
| update | 85.00 |
| ı-des-01 | 7.00 |
| update | 7.00 |
| Aug 14, 00:54-00:55 | 85.00 |
| ›-des-02 | 85.00 |
| update | 85.00 |
| Aug 14, 00:56-00:57 | 85.00 |
| -des-01 | 85.00 |
| update | 85.00 |
| -des-01 | 85.00 |
| update | 85.00 |
| ı-des-02 | 85.00 |
| update | 85.00 |
| Aug 14, 00:57-00:58 | 161.00 |
| -des-01 | 161.00 |
| update | 161.00 |
| withdraw | 161.00 |

MEASURE

Distinct Prefix ▾

BGP RIB

| | |
|---|---|
| ☑ loc | 286.00 |
| □ adj_in_post | 85.00 |

RD

| | |
|---|---|
| 1:10.187.97.22:66 | 33.75 k |
| 1:10.187.97.36:1 | 33.73 k |
| 1:10.187.97.22:0 | 26.00 k |
| 1:10.187.97.25:0 | 26.00 k |
| 1:10.187.97.36:2 | 26.00 k |
| 1:10.187.97.33:1 | 16.65 k |
| 0:6837:2215 | 13.00 k |
| 0:6837:2214 | 12.95 k |
| 1:10.187.97.33:2 | 11.96 k |

ECOMMS

| | |
|---|---|
| RT: :1100110164 | 286.00 |
| ? | 14.00 |

PEER IP

| | |
|---|---|
| 0.0.0.0 | 286.00 |

BGP NEXTHOP

| | |
|---|---|
| ::1 | 159.00 |
| ::1 | 85.00 |
| .72 | 63.00 |
| ::1 | 40.00 |
| ::1 | 40.00 |
| ::1 | 3.00 |

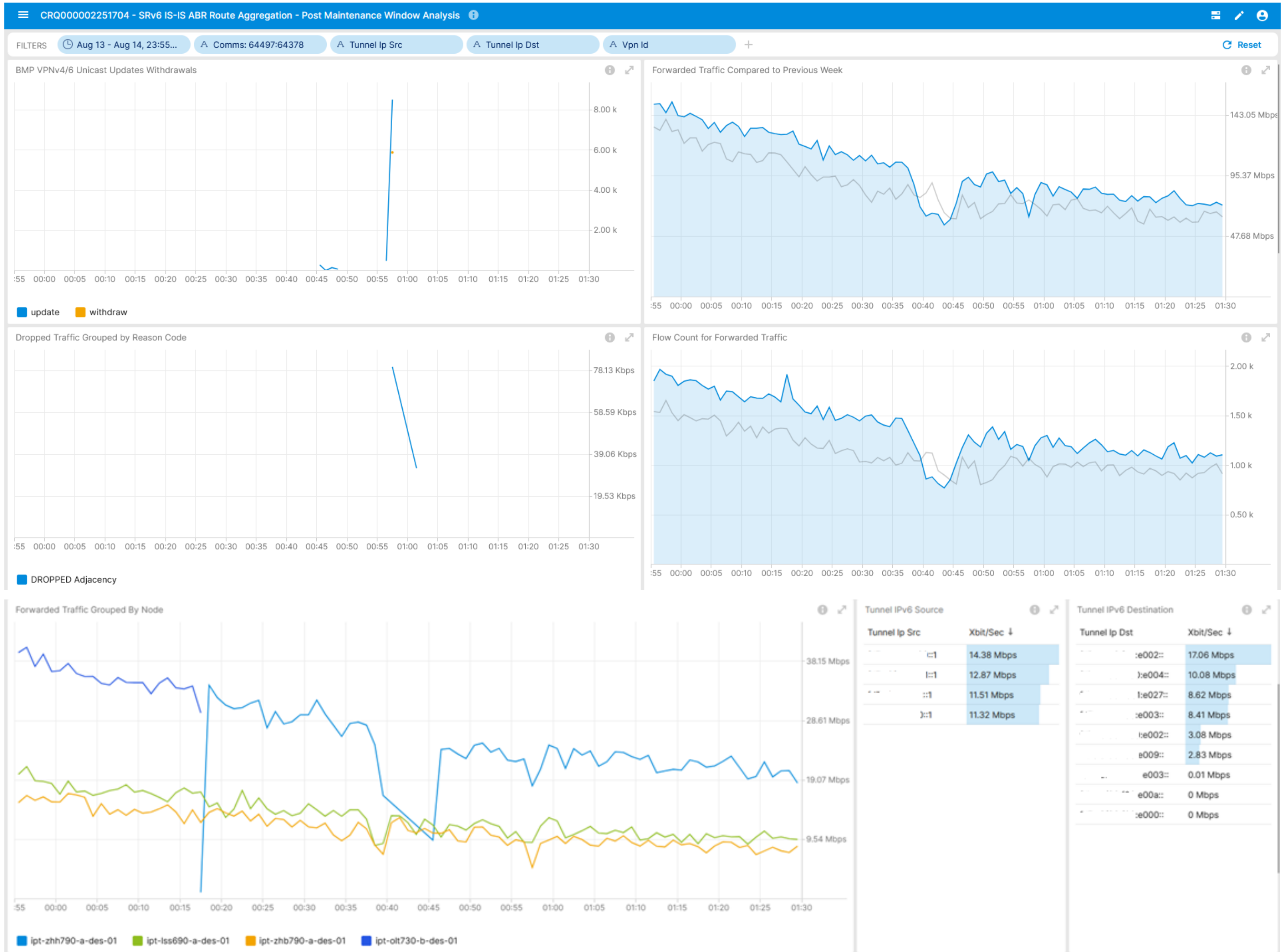
+ Add dimension

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



CRQ000002251704 - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Aug 13 - Aug 14, 23:55... | Comms: 64497:64378 | Tunnel Ip Src | Tunnel Ip Dst | Vpn Id

Tunnel IPv6 Source

| Tunnel Ip Src | Xbit/Sec ↓ |
|---|---|
| c::1 | 14.38 Mbps |
| l::1 | 12.87 Mbps |
| ::1 | 11.51 Mbps |
| )::1 | 11.32 Mbps |

Tunnel IPv6 Destination

| Tunnel Ip Dst | Xbit/Sec ↓ |
|---|---|
| :e002:: | 17.06 Mbps |
| ):e004:: | 10.08 Mbps |
| l:e027:: | 8.62 Mbps |
| :e003:: | 8.41 Mbps |
| !:e002:: | 3.08 Mbps |
| e009:: | 2.83 Mbps |
| e003:: | 0.01 Mbps |
| e00a:: | 0 Mbps |
| :e000:: | 0 Mbps |

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

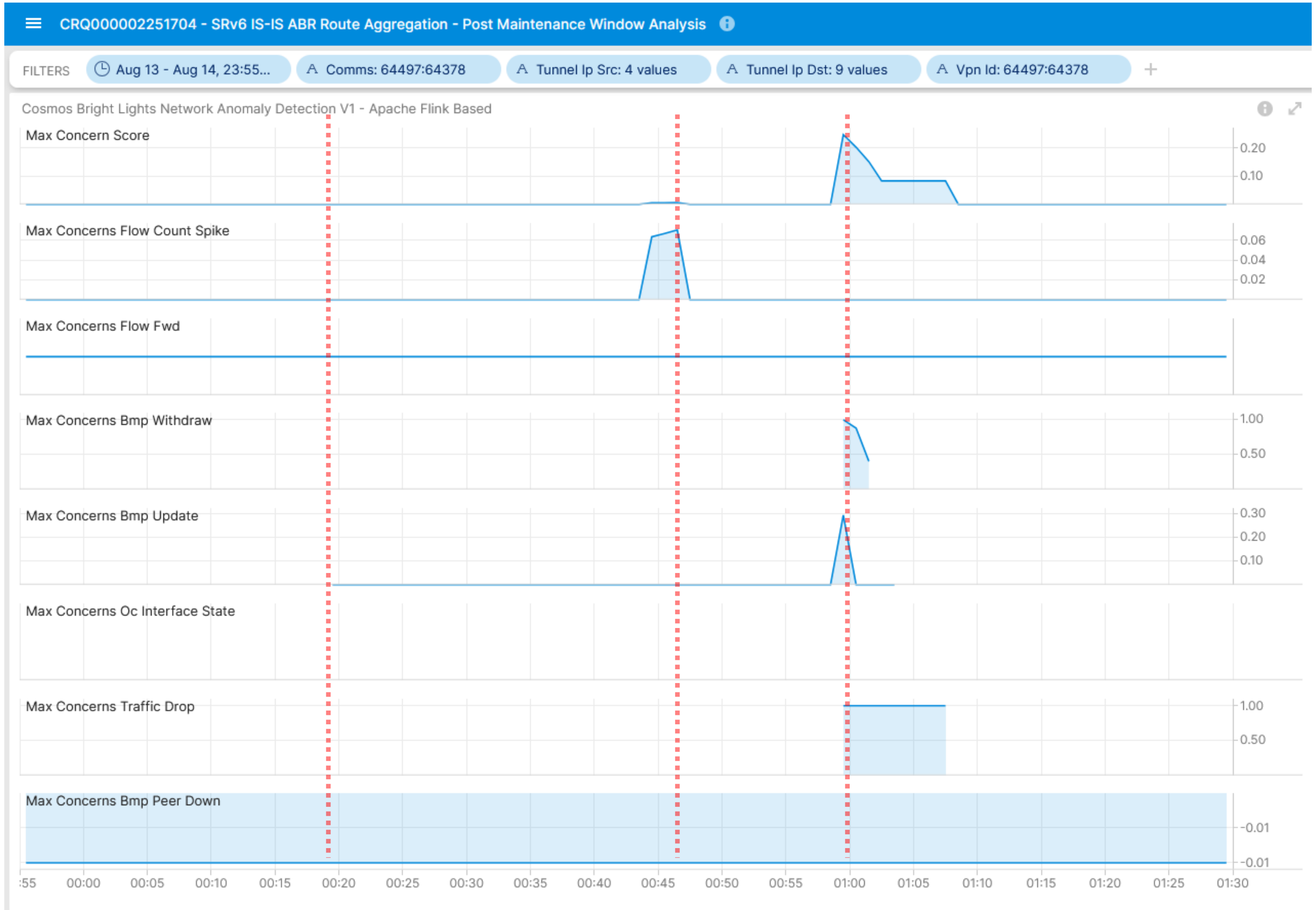
**Logical Connection 64497:64378 SRv6 L3 VPN Overlay and Underlay Operational Metrics**

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

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

Real-Time Streaming under Development

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



CRQ000002251704 - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Aug 13 - Aug 14, 23:55... | Comms: 64497:64378 | Tunnel Ip Src: 4 values | Tunnel Ip Dst: 9 values | Vpn Id: 64497:64378

Cosmos Bright Lights Network Anomaly Detection V1 - Apache Flink Based

♕ **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.**

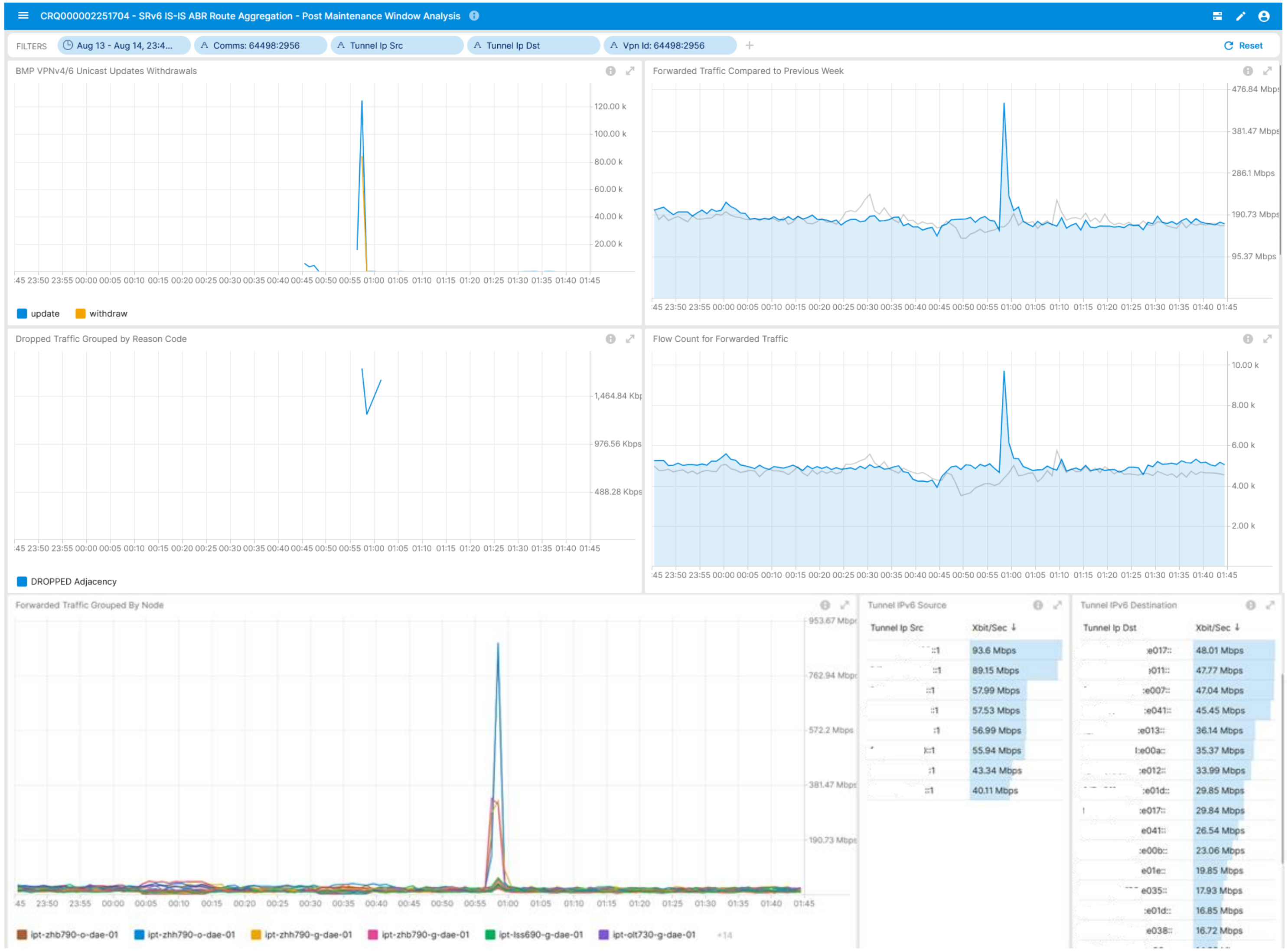
♕ **Missing Traffic check recognized traffic loss.**

♕ **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



CRQ000002251704 - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Aug 13 - Aug 14, 23:4... | Comms: 64498:2956 | Tunnel Ip Src | Tunnel Ip Dst | Vpn Id: 64498:2956 | Reset

BMP VPNv4/6 Unicast Updates Withdrawals

Forwarded Traffic Compared to Previous Week

Dropped Traffic Grouped by Reason Code

Flow Count for Forwarded Traffic

Forwarded Traffic Grouped By Node

Tunnel IPv6 Source

| Tunnel Ip Src | Xbit/Sec ↓ |
|---|---|
| ::1 | 93.6 Mbps |
| ::1 | 89.15 Mbps |
| ::1 | 57.99 Mbps |
| ::1 | 57.53 Mbps |
| :1 | 56.99 Mbps |
| ):1 | 55.94 Mbps |
| :1 | 43.34 Mbps |
| ::1 | 40.11 Mbps |

Tunnel IPv6 Destination

| Tunnel Ip Dst | Xbit/Sec ↓ |
|---|---|
| :e017:: | 48.01 Mbps |
| ɔ011:: | 47.77 Mbps |
| :e007:: | 47.04 Mbps |
| :e041:: | 45.45 Mbps |
| :e013:: | 36.14 Mbps |
| l:e00a:: | 35.37 Mbps |
| :e012:: | 33.99 Mbps |
| :e01d:: | 29.85 Mbps |
| :e017:: | 29.84 Mbps |
| e041:: | 26.54 Mbps |
| :e00b:: | 23.06 Mbps |
| e01e:: | 19.85 Mbps |
| e035:: | 17.93 Mbps |
| :e01d:: | 16.85 Mbps |
| e038:: | 16.72 Mbps |

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

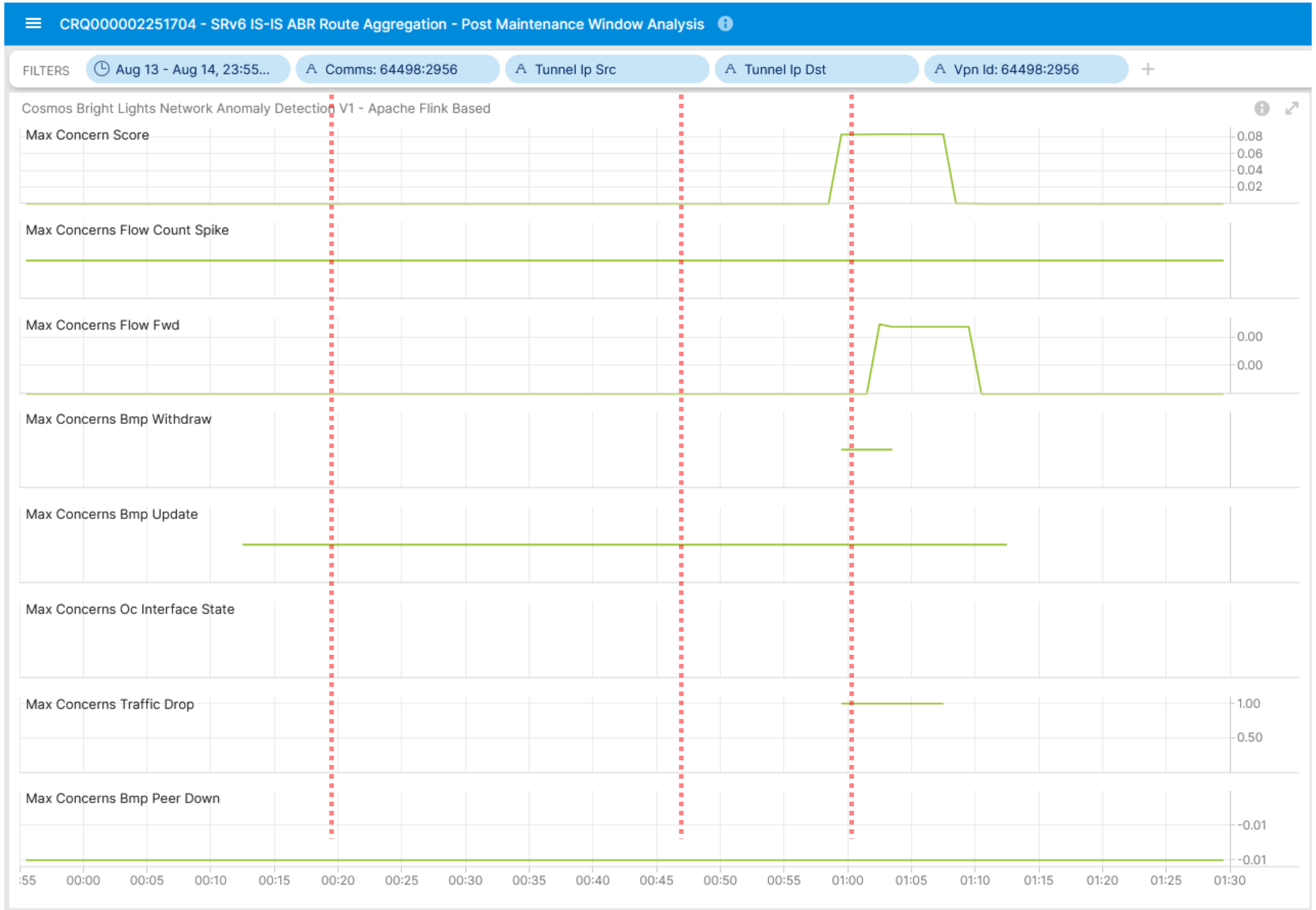
**Logical Connection 64498:2956 SRv6 L3 VPN Overlay and Underlay Operational Metrics**

# 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**



CRQ000002251704 - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Aug 13 - Aug 14, 23:55... | Comms: 64498:2956 | Tunnel Ip Src | Tunnel Ip Dst | Vpn Id: 64498:2956

Cosmos Bright Lights Network Anomaly Detection V1 - Apache Flink Based

SOS **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.**

SOS **Missing Traffic check did not recognize traffic blackholing.**

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

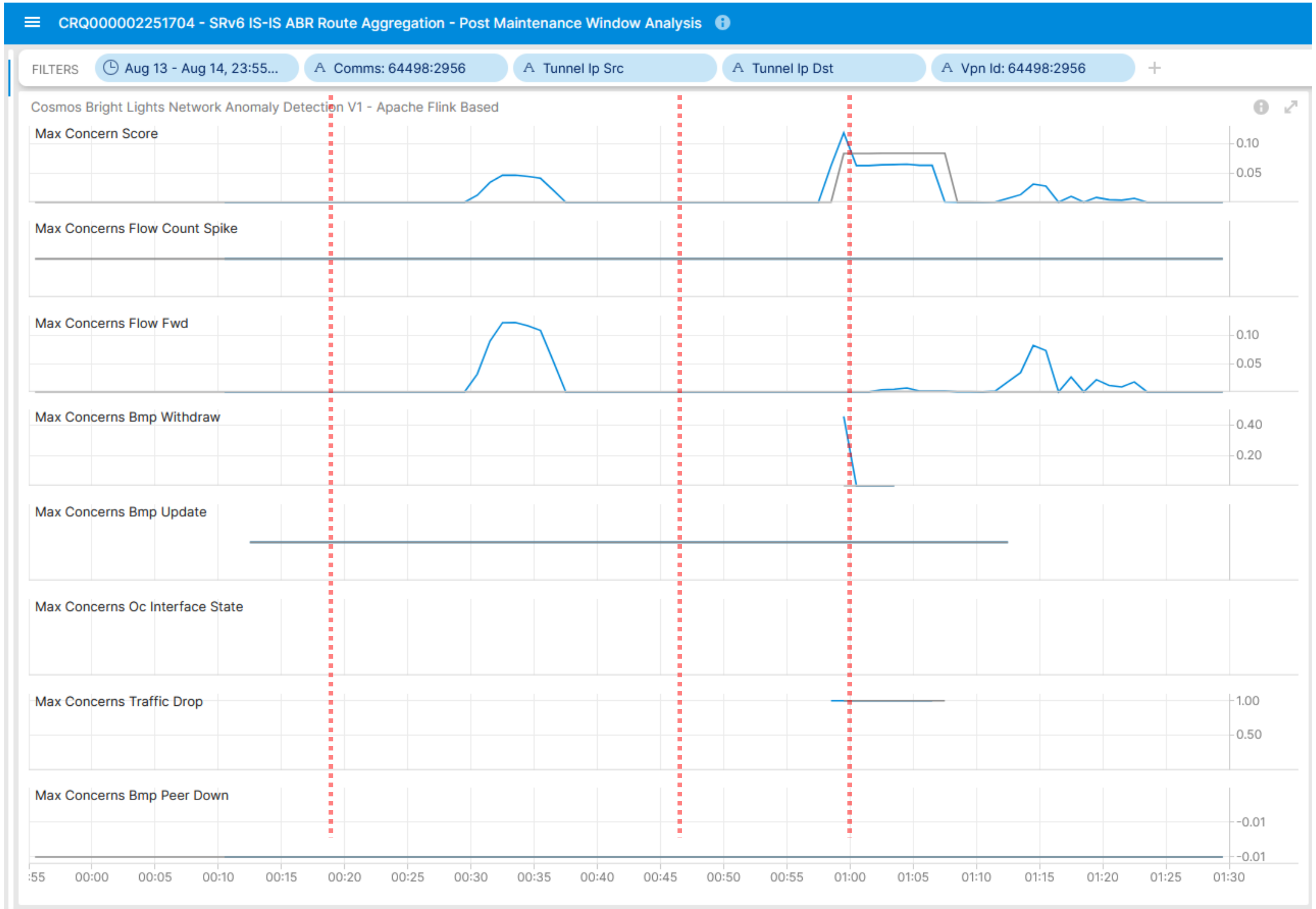
♕ **Overall: 1 out of 6 checks have detected the BGP topology change. Real-time streaming implementation.**
**Auto profiling under implementation.**

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

## 64497:2956 SRv6 L3 VPN – Anomaly Detection Replay

Concern Score: **0.12**
Flow Count Spike: **0.00**
Missing Traffic: **0.12**
Traffic Drop: **1.00**
BMP Update/Withdrawal: **0.00/ 0.46**

Real-Time Streaming under Development



CRQ000002251704 - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Aug 13 - Aug 14, 23:55... | Comms: 64498:2956 | Tunnel Ip Src | Tunnel Ip Dst | Vpn Id: 64498:2956

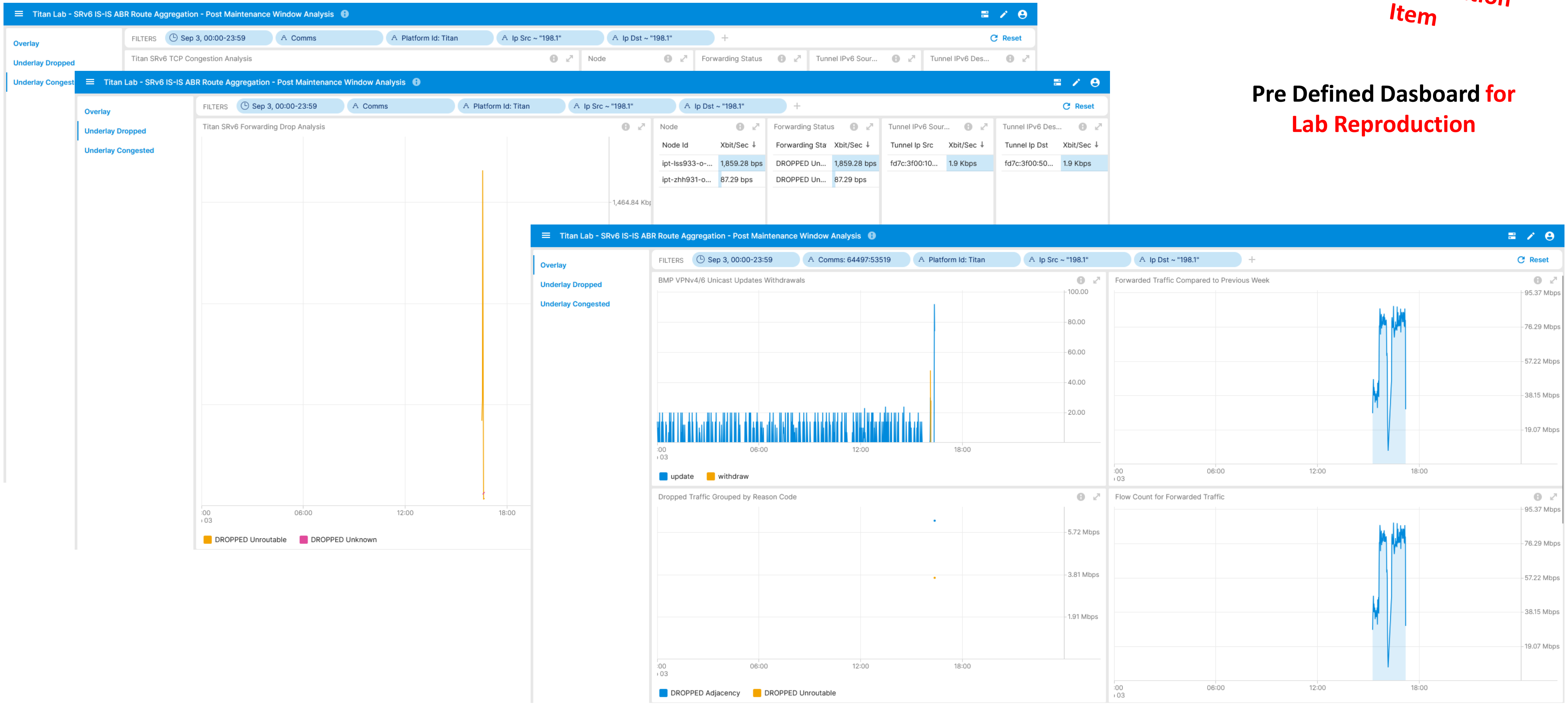
Cosmos Bright Lights Network Anomaly Detection V1 - Apache Flink Based

- **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 recognized traffic blackholing.**
- **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 exceeds expectations.**

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

## Lab Repro In Progress

Reproduction Partial Successful
Identified Root Cause and Configuration Item



Titan Lab - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Sep 3, 00:00-23:59 · Comms · Platform Id: Titan · Ip Src ~ "198.1" · Ip Dst ~ "198.1"

Titan SRv6 Forwarding Drop Analysis

| Node Id | Xbit/Sec ↓ |
|---|---|
| ipt-lss933-o-... | 1,859.28 bps |
| ipt-zhh931-o... | 87.29 bps |

| Forwarding Sta | Xbit/Sec ↓ |
|---|---|
| DROPPED Un... | 1,859.28 bps |
| DROPPED Un... | 87.29 bps |

| Tunnel Ip Src | Xbit/Sec ↓ |
|---|---|
| fd7c:3f00:10... | 1.9 Kbps |

| Tunnel Ip Dst | Xbit/Sec ↓ |
|---|---|
| fd7c:3f00:50... | 1.9 Kbps |

Titan Lab - SRv6 IS-IS ABR Route Aggregation - Post Maintenance Window Analysis

FILTERS: Sep 3, 00:00-23:59 · Comms: 64497:53519 · Platform Id: Titan · Ip Src ~ "198.1" · Ip Dst ~ "198.1"

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 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 as intended 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 too high to ensure network being monitored in all aspects.
- 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?

- False positive due to partially missing profiling (work in progress) for flow aggregation. Consider profiling for BMP update/withdrawals as well.
- Missing IS-IS control plane visibility. This would have helped to understand the routing topology state changes. 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.
- Missing Forwarding plane path visibility (Passive Hybrid Type 1). 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, changes in VPNv4/6 unicast paths would have been visible. Reducing the 1min granularity in TSDB would have helped to detect race condition.
- The connectivity service, the network relationship, was not taken 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.