flowEye™

A real time In-band Network Telemetry and Analytics product suite

Overview

Kaloom's flowEye™ In-band Network Telemetry (INT) and Analytics solution is a key product offering that complements the Software Defined Fabric™ and Cloud Edge Fabric™ products[1]. The solution comprises a real-time In-band Network Telemetry component which serves the role of data collection via hardware or software based INT sensors, and an analytics component (Kaloom's or a customer owned third party solution) which aggregates the collected data, performs data analysis, and displays it via different views in the dashboard. The solution leverages the capabilities of the P4 programmable ASIC based switches to obtain granular, real-time insight of the network state regarding key metrics pertaining to packets based on actual traffic and their flow as they traverse the network.

Figure 1 below provides a pictorial overview of the in-band telemetry data as it gets collected, aggregated, analysed and visualized.

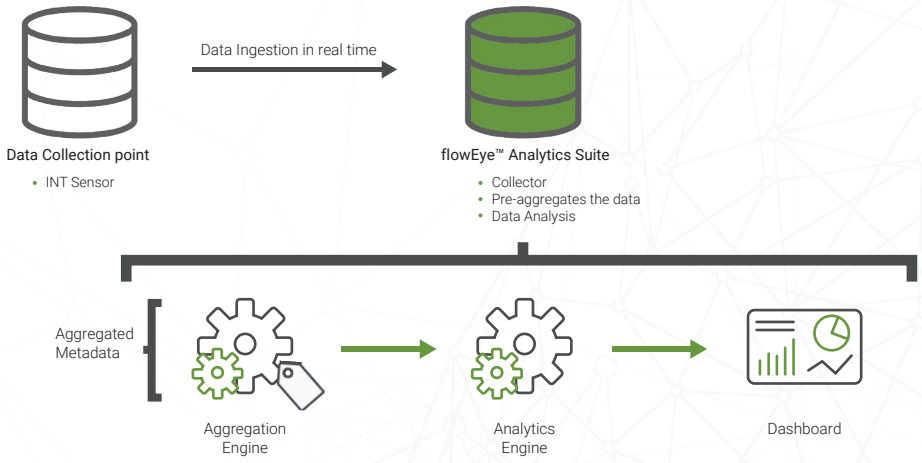

Figure 1: Feeding Data into the Analytics Suite

The solution offers benefits over other more traditional network troubleshooting and diagnostic methodologies that either employ a passive, non real-time statistical/sampled method (i.e., SNMP, NetFlow, sFlow, IPFIX) for network monitoring or an active, real-time synthetic method (i.e., 802.1ag, TWAMP) using expensive equipment to push artificial test traffic into the environment typically with the same forwarding criteria as the user/service traffic being monitored, and then measuring the resulting performance; which as expected would be less than optimal due to the addition of test traffic and its impact of increasing the total packet latency through the network. In general, these traditional network monitoring methods suffer from being expensive, inefficient, providing very little visibility and control, and ineffective in capturing key networking occurrences (i.e., microbursts etc.). In comparison, Kaloom's INT methodology provides greater knowledge about the state of the network in real time, by processing raw packet data to derive faster, deeper, and more accurate analytics without the need to buy additional equipment, as well as being enabled to function as a fully closed loop system[2].

[1]For more information on the Software Defined Fabric™ and Cloud Edge Fabric, please refer to: https://www.kaloom.com/product-collateral
[2]See table 2 for more information

Table 1 below outlines the various components within the flowEye platform, the functions they perform, and where they are deployed.

Product	Components	Functions	Deployment
flowEye™ Platform	INT Virtual Software Sensor	• Packet Capture • Metadata Extraction • Timestamping • Fingerprinting	• Server + NIC • Embedded Software
	INT Virtual Hardware Sensor	• Packet Capture • Metadata Extraction • Timestamping • Fingerprinting	• Embedded in Leaf/Spine Switches • P4 Based
	flowEye Aggregator	• Metadata Aggregtion • Flow Generation	• Any x86 Hardware
	flowEye Analyzer	• Flow Statistics • Alerts	• Any x86 Hardware
	flowEye Console	• Dashboard • Analysis • Alerts	• Web Browser

Table 1: flowEye Components

flowEye collects and reports network state via advanced timing-based algorithms by collecting in-band network telemetry data (i.e., metadata) and feeding it to a backend analytics engine for detailed analysis. The INT solution implements packet mirroring techniques to carry out a "Postcard" mode of operation that is performed in the data plane, without impacting the control plane. In the postcard mode each spine and leaf switch can generate a telemetry report to send directly to the collector/monitoring server. Data packets contain header fields that are interpreted as "telemetry instructions" by network devices. INT data can be collected from multiple packets in real time based on programmable selection criteria (a.k.a. Watch List Rules) and customer defined sampling rates.

flowEye enables advanced packet tracing capabilities in real time ("traceroute") of the network route. The networking nodes along the path use the INT instructions to tell an INT capable device what state to collect and write into the packets as it transits the network. Using this information provides better granularity and facilitates Root Cause Analysis, whereby network problems can be pinpointed, and corrective actions can be taken.

Figure 2 provides a high-level architectural overview to illustrate Kaloom's implementation of the "Postcard" method for telemetry data reporting for INT. In brief, INT requires minimal configuration focused on setting-up the "watch list rules" that specify all traffic to be monitored. In the scenario shown, INT is configured to monitor traffic originating from Host A to Host B. The network nodes are set to forward telemetry information to Controller 1 as shown by the dotted line arrows. Within the INT process, the ingress switch (Leaf 1) performs three main tasks, namely; it identifies flows based on a set of rules, marks packets for monitoring, and finally, it generates postcards for all marked packets. Any other network switch in the path (spine and egress leaf switches) that detect marked traffic also generate postcards.

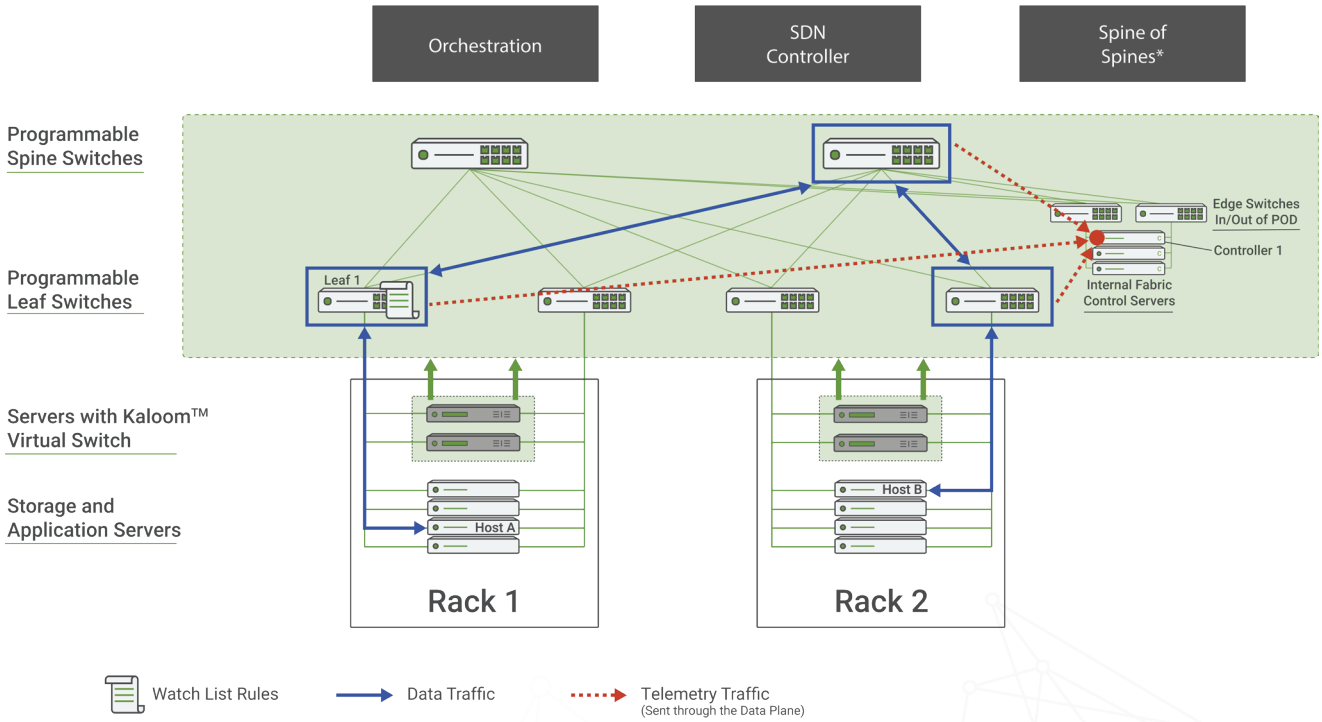

Figure 2: In-Band Network Telemetry Implementation

The data collected can be further analyzed by the analytics engine and presented in an advanced dashboard providing intuitive, real-time insights into hard-to-find problems. The dashboard creates an accurate, real-time map of network activity. All collected and processed measurement data is accessible from a consolidated User Interface (UI) via a browser that enables the visualization of network measurements on a hop-by-hop, segment-by-segment, or end-to-end basis.

Figure 3 graphically represents the various views within the analytics solution that enable packet and flow visibility.

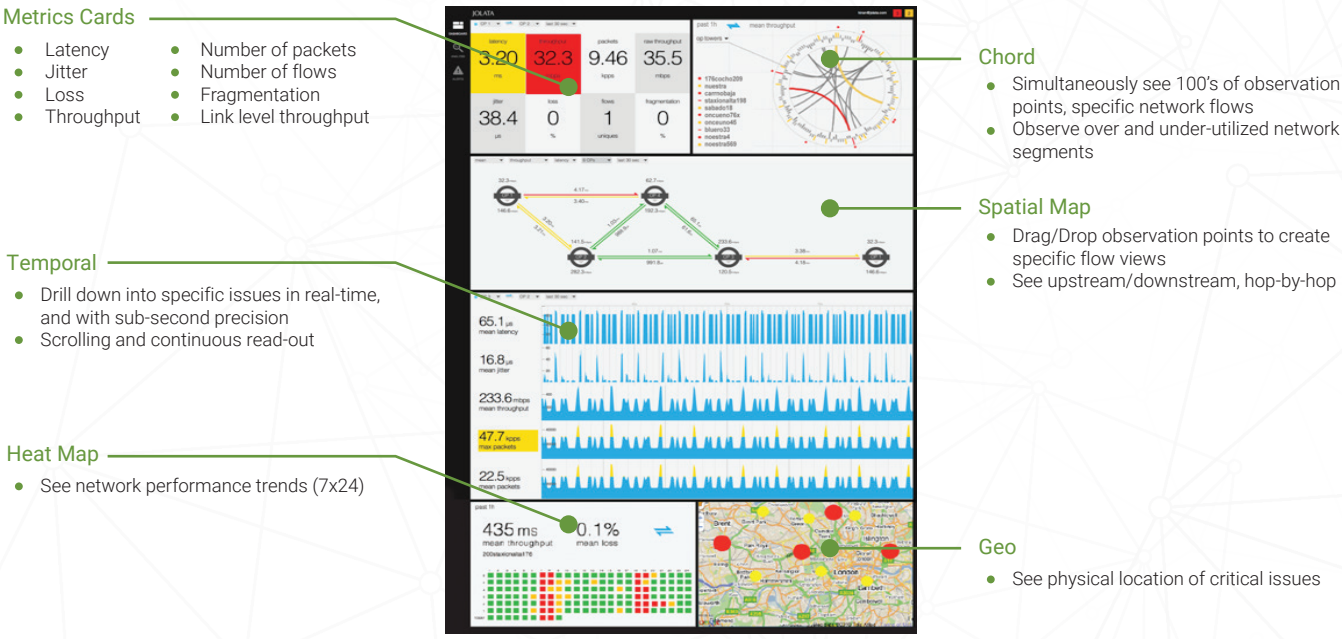

Figure 3: Dashboard Views

Table 2 on the following page lists the business benefits offered by Kaloom's In-band Network Telemetry and Analytics product offering.

Feature	Benefits
flowEye™ In-band Network Telemetry & Analytics Solution	❯ A complete suite of integrated INT and Analytics for Software Defined Fabric and Cloud Edge Fabric • Industry's first real time In-band Network Telemetry Solution • Enables the ability to "see what others miss, or can't see at all" ❯ Enables today's modern data centers to be equipped with the most cutting-edge real-time network monitoring and analytics tool • Enables customers to visualize/find/fix infrastructure issues across multi data center environments • Correlates applications to specific network flows • Displays point, segment, and transactional metrics in less than 5 seconds • Visualizes results with 100ms precision ❯ Measures actual traffic, not sampled or synthetic • Monitor up to every packet, every flow in real-time ❯ AI driven • Enables self-healing and auto remediation of anomalies and problems ❯ Enables self driving data centers and networks • Enables customers to build "self driving" data center networks and to build closed loop systems that encompass orchestration, analytics and self-healing/automatic remediation for better operation and lower OPEX cost ❯ Segment Analytics for better RCA • Provides a detailed view of each link/segment from source to destination • Fine-granular view of the path gives faster RCA ❯ Provides detailed visibility and RCA of OpenStack/Kubernetes/OpenShift to Networking • Enables distributed application framework and micro services visibility ❯ Avoids the need to buy additional expensive, specialized equipment and the latency they add in measuring network traffic parameters • Fully integrated into the cloud edge fabric and software defined fabric • Save at least 2-3x in CAPEX to not have to buy separated monitoring or packet brokering hardware products ❯ Supports migration and legacy services view • Can instantiate software-based sensors in legacy PODs to get a common view of the SLA/KPI for the services and application for Kaloom PODs and legacy PODs • Uses hardware and software-based sensors and enables networks to achieve higher performance levels and lowers OPEX costs via easier deployments and more powerful troubleshooting capabilities ❯ Facilitates "always accessible services" and highest possible network availability • Enables root cause analysis by helping to pinpoint networking problems via the aggregation of telemetry data and the generation of detailed reports about the network state ❯ Enables the support of newer applications enabled by 5G, IIoT (i.e., self driving cars, remote surgery, Augmented Reality/ Virtual Reality, etc.) • Enables customers to deploy a network monitoring solution that is ideally suited to the low-latency applications of 5G

Table 2: Dashboard View Types & Measurements Visualized

MBUZZ Europe

Kaloom's Exclusive Partner in Europe

Contact Us

- contact@mbuzzeurope.com
- www.mbuzzeurope.com
- linkedin.com/company/mbuzzeurope
- twitter.com/MBUZZEurope

Headquarters

355 Rue Peel, Suite 403
Montreal, Quebec, Canada
H3C 2G9

www.kaloom.com
info@kaloom.com