Packet based Metadata: The Key to Uncovering "Unknown Unknowns" in Network Observability and Security Monitoring

By **Mark Grodzinsky**, Chief Product and Marketing Officer

In today's dynamic network environments, traditional MELT telemetry (metrics, events, logs, and traces) falls short when uncovering "unknown unknowns"—unforeseen issues that can cripple network performance and endanger network security. Packets and metadata generated from the packets data offer a more granular, real-time view, providing the level of detail necessary to identify these undetected anomalies and veiled vulnerabilities.

The Shortcomings of MELT Telemetry

While MELT telemetry can alert you to "known unknowns"—anticipated issues you've prepared for—its reliance on aggregation and predefined triggers leaves it blind to unexpected network events or attacks. Metrics and logs may highlight a symptom, such as increased latency or packet loss, but they rarely offer the full picture of why it occurred.

- **Aggregated and Summarized Data:** MELT telemetry, particularly metrics, often aggregates data, leading to a loss of crucial details. For example, a spike in traffic might show up in a metric, but it doesn't explain where the traffic came from or why it occurred.
- Reactive, Not Proactive: Logs and events are designed to capture issues after they have already occurred. To log something, you must have anticipated the problem, limiting MELT's ability to capture unanticipated or novel issues in real-time.
- **Limited Root Cause Analysis:** High-level logs and traces offer only a partial view of incidents, lacking the granularity needed to trace issues back to their source.
- **Blind Spots for Short-Term Anomalies:** Critical events such as packet drops or latency spikes will happen too quickly for MELT telemetry to detect.

The Actual Packets: A Complete View of Network Traffic

Packets solve these problems by providing a granular, real-time view of all network traffic. Unlike MELT telemetry, packet-based metadata doesn't rely on predefined events or logs, making it ideal for discovering unknown issues. Specifically, using the actual packets enable:

- **Granular Insights for Root Cause Analysis:** The packets include detailed information about each packet, such as timestamps, protocol types, and source/destination IPs. This allows network engineers to trace issues to the exact moment they occurred.

- **Real-Time Monitoring:** The packets allow you to gain proactive, real-time insights into network traffic, helping to prevent issues from escalating into major outages or breaches.
- **Detection of Microbursts and Latency Spikes:** Packets capture the fleeting but impactful network anomalies, like microbursts, that can severely impact performance but are missed by traditional MELT telemetry.
- **Comprehensive Security Monitoring:** By capturing every packet and using them to create accurate metadata enables detailed forensics, helping security teams trace malicious activities to their origin and respond more effectively to breaches.

Discovering the Unknown Unknowns

The true value of the packets lies in its ability to uncover the **"unknown unknowns"**—unanticipated issues that MELT telemetry can't detect because no predefined trigger or log exists for them. While MELT data can track **"known unknowns,"** packets offer a complete, unfiltered view of network traffic, allowing teams to identify new and emerging issues before they cause widespread impact.

For example, a security breach caused by an unfamiliar vulnerability may bypass traditional logs or event triggers, but the packets capture the full sequence of actions, providing crucial context for investigation and mitigation.

Real-World Use Cases using the Packets

- **Performance Optimization:** Helping identify specific issues such as congestion, packet loss, and traffic bursts, leading to faster and more effective performance tuning.
- **Security Forensics:** Security teams can reconstruct attacks with full packet data, enabling quicker response times and better threat detection.
- **Microburst Detection:** Short-lived anomalies, such as microbursts, can be detected and analyzed, which is crucial in industries like financial services or real-time communications where milliseconds matter.

Conclusion

While MELT telemetry provides useful high-level insights, it lacks the granularity needed to fully understand the complex behaviors in modern networks. The packets and the generated metadata fill that gap by offering comprehensive, real-time visibility into every packet traversing the network. This detailed view is essential for discovering unknown unknowns, reducing Mean-Time-to-Resolution, and enhancing both network performance and security.

Do not ignore the actual packets from your observability and security strategy because they are crucial for staying ahead of unforeseen issues and ensuring network resilience in today's high-speed, high-stakes environments. By relying on packet-level data, organizations can move beyond monitoring what they know to proactively uncovering and addressing what they don't.

About cPacket Networks

cPacket Networks de-risks IT I&O through network-aware service and security assurance across hybrid and multi-cloud environments. Our AIOps-ready Intelligent Observability Platform provides single-pane-of-glass analytics and deep network visibility required for complex IT environments enabling Fortune 500 organizations around the world to keep their business running. cPacket solutions are fully reliable, tightly integrated, and consistently simple. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased service agility, enhanced experience assurance, and faster transactional velocity. Learn more at **cpacket.com**.

BL-100824