Application Metadata Intelligence NetFlow

Challenges of NetFlow Generation

As enterprise networks continue to grow and network speeds continue to increase, the ability for business-critical appliances to consume and analyze the additional data is, by contrast, diminishing in equal proportion. Threat complexity, for instance, is requiring security devices to take on more complex analytics; but it is also straining already scarce compute on appliances that can barely match 10Gb speed — let alone 25G, 40Gb, 100Gb, or higher.
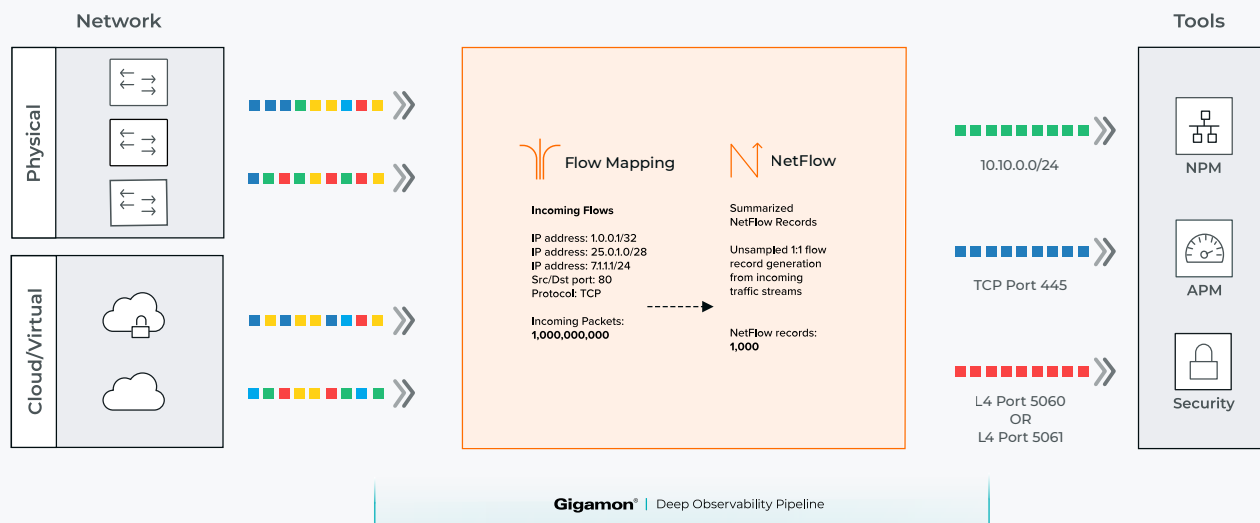
Figure 1. NetFlow generation.

In short, the problem is too much data, but too little compute. And the answer? Metadata.

NetFlow is one form of metadata. This Layer 2–4 flow data can increase visibility into traffic across systems and be used to build relationships and usage patterns between nodes on the network — but only if produced the right way.

While routers and switches are capable of generating NetFlow flow data, they were not designed to do so for every packet. This creates challenges and limitations. Not only is router- or switch- generated Netflow sampled, but it may be non-standard and inconsistent in format, and requires processing overhead that can introduce service degradation, latency, and packet drops. Further, the type of sampling employed is not well controlled, with:

- **Packet-based sampling**, resulting in incomplete session flow records
- **Session tracking limits being exceeded**, thereby missing possibly critical or important flows
- **Packet or session processing rate limits being exceeded**, thereby resulting in incomplete session flow records, possibly critical/important flows being missed, or both

And what makes it even more challenging is that different switch vendors, switch families/models, and switch generations all have different limitations regarding NetFlow generation. The result is a messy, inconsistent, spotty, and unreliable collected set of network flow data.

What's more, even if these processing issues were able to be resolved, NetFlow up to version 9 is still only Layers 2 to 4.

The Gigamon Solution

From incoming traffic streams, Gigamon NetFlow can generate Layer 2–4 flow data. And the key differentiators and benefits? This NetFlow is unsampled; it supports a range of NetFlow formats, including NetFlow versions 5 and 9, IPFIX (NetFlow v10), and CEF for seamless integration with an unlimited number of standards-based collectors, storage devices, and SIEMs; and it is done without causing any processing overload or performance degradation in the network. While, AMI can be used for Layer 7 metadata in addition to NetFlow.

Gigamon Flow Mapping® technology can also be used to pick and choose from flows to generate NetFlow while, at the same time, sending the original packets to other monitoring tools. Operators can also export NetFlow records to multiple collectors concurrently, creating a single flow source for business-critical management applications such as security, billing, capacity planning, and more.

The Gigamon Deep Observability Pipeline establishes a scalable framework to deliver pervasive, flow-level visibility across networks and data centers within enterprises, government organizations, and service provider environments to help users accurately design, engineer, optimize, and manage their network infrastructure.

The solution delivers the following capabilities:

- Ability to generate unidirectional records (Netflow v5/v9) and bidirectional records (IPFIX and CEF)
- Support for IP fragmentation
- Support for dual-stack traffic (IPv4/IPv6)
- Ability to generate metadata for tunneled (L2GRE, VXLAN, GTP and MPLS) traffic
- Can be combined with Slicing and Masking in addition to De-duplication GigaSMART Operation.

Key Features and Benefits of NetFlow with GigaSMART

Features	Benefits
Deep observability with NetFlow generation across the entire network	Security and performance monitoring tools get complete view of the network versus isolated views of individual network segments generated by a specific router or switch
High-throughput out-of-band NetFlow solution	No performance impact of NetFlow generation on production routers and switches
Unsampled 1:1 NetFlow generation on every packet	Complete and precise picture of network activity for security monitoring without loss of fidelity incurred from sampled NetFlow generation
Support for a wide range of NetFlow export formats – v5, v9, IPFIX, and CEF	Compatibility with legacy and next-generation NetFlow collectors
Ingress filtering on Layer 2, Layer 3, and Layer 4 headers using Gigamon Flow Mapping	Generate flow statistics for specific networks and applications
Support for up to five collectors with customizable templates and filters	Leveraging multiple vendors for security and application monitoring

NetFlow generation is supported by GigaVUE® Cloud Suite for processing in public or private cloud environments, and by GigaVUE HC Series for processing in on-premises environment.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding the Gigamon Limited Warranty and its Product Support and Software Maintenance Programs, visit gigamon.com/support-and-services/overview-and-benefits.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.