Legacy 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.

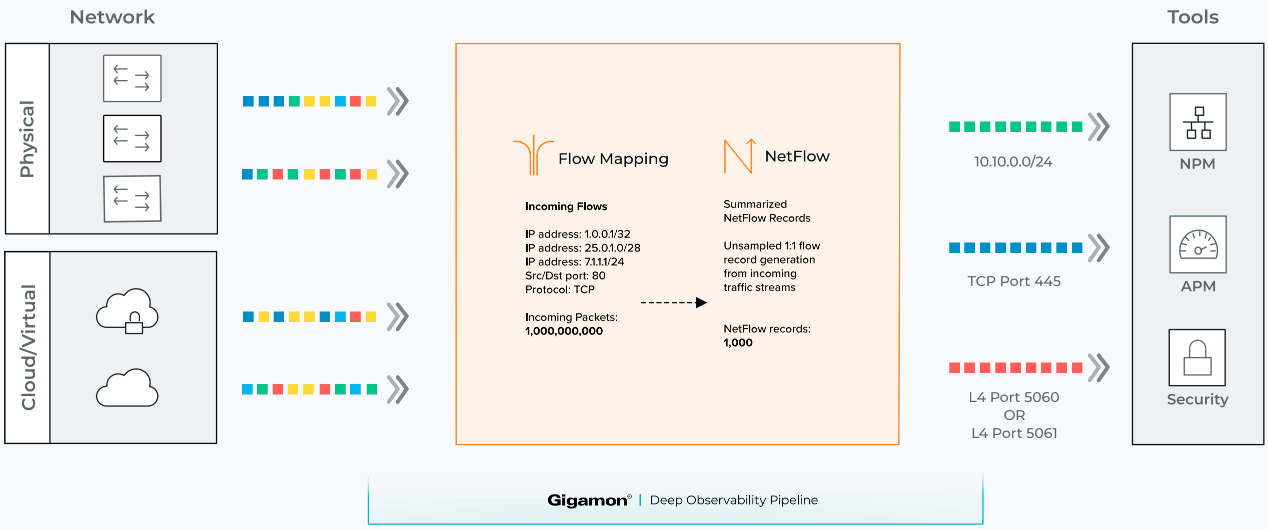

Figure 1. NetFlow generation.

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 is also 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 2-4. Organizations also need some Layer 7 application-level metadata to achieve pervasive, actionable visibility and successful analysis.

The Gigamon Solution

From incoming traffic streams, Gigamon NetFlow can generate both Layer 2–4 flow data and important Layer 7 metadata. 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.

Gigamon has extended IPFIX to include not only standard information about traffic — like source and destination IP addresses and ports — but also key application-specific extensions, such as DNS, URL, and HTTP response codes, to name a few. To eliminate the impact and risk of expending expensive production network resources in generating this data, Gigamon has enabled operators to offload network flow data generation to an out-of-band solution within the Gigamon Deep Observability Pipeline, as well as obtain additional key application metadata elements.

Patented Gigamon Flow Mapping® technology can also be used to pick and choose from flows to generate NetFlow and metadata statistics while, at the same time, sending the original packets to other monitoring tools. Operators can also export NetFlow records plus the application metadata to multiple collectors concurrently, creating a single flow source for business-critical management applications such as security, billing, capacity planning, and more. And finally, they can filter exported flows so that collectors only receive the specific records relevant to them.

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.

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

Key Metadata Extensions

Extension	Fields Extracted	Benefits
DNS	• dnsIdentifier • dnsOpCode • dnsResponseCode • dnsQueryName • dnsResponseName • dnsResponseTTL • dnsResponseIPv4Addr • dnsResponseIPv6Addr	• Uncover domain lookups for malicious command and control (C&C) servers • Identify endpoints potentially infected with bots • Identify suspicious DNS servers that have low time-to-live (TTL) values • Identify rogue DNS servers in the network
URL	URL from method types: • HTTP GET • POST • PUT • DELETE • HEAD	• Identify malicious communications to C&C servers • Identify potential SQL and other OWASP vulnerabilities from URLs • Identify productivity and compliance violations using URL metadata

Key Metadata Extensions, Continued

Extension	Fields Extracted	Benefits
HTTP response codes	HTTP response codes: • 100–199 (informational) • 200–299 (success related) • 300–399 (redirection) • 400–499 (client requests) • 500–599 (server related)	• Baseline of HTTP codes to uncover anomalous behavior patterns • Identify excessive redirections (3XX codes) that could point to compromise of internal servers • Identify excessive 4XX codes that could signal potential denial of service attacks and communications to C&C servers from infected hosts
Certificates	• sslCertificateSubject • sslCertificateValidNotBefore • sslCertificateValidNotAfter • sslCetificateSerialNumber • sslCertificateSignatureAlgorithm • sslCertificateSubjectPubAlgorithm • sslCertificateSubjectPubKeySize • sslCertificateSubjectAltName • sslServerNameIndication • sslServerVersion	• Identify expired certificates in the network • Identify self-signed certificates in the network • Identify certificates using weak cipher algorithms • Identify mismatches in certificate subject fields (if subject field does not match website domain name)
CDP	• Device ID • Port ID • TTL • Platform • SW Version • Native VLAN ID • Capabilities • Network Prefix Address • Network Prefix Mask • Interface Address • Management Address	• Identify source or destination machine type instead of IP address (e.g., Catalyst 6K switch) • Reduce time to resolution by identifying physical location of traffic within the network
LLDP	• Chassis IP • Port ID • TTL • Port Description • System Name • System Description • Management Address • Capabilities Available • Capabilities Enabled • VLAN Name • Port VLAN ID • Management VLAN ID • Link Aggregation ID • Link Aggregation Status • MTU	• Identify source or destination machine type instead of IP address • Reduce time to resolution by identifying physical location of traffic within the network
SIP	Sender and receiver information from • INVITE • ACK • BYE • REGISTER • OPTIONS • CANCEL request types	Get source and destination caller information in addition to IP addresses for a SIP call

NetFlow generation is supported by GigaVUE HC Series for processing physically on-premises.

If more extensive application metadata is required, this is supported on the same platforms using the Application Metadata Intelligence GigaSMART® application.

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 harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves 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 worldwide. To learn more, please visit gigamon.com.

For more information about Gigamon, or to contact a local representative, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com