NetFlow and IPFIX Generation

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.

In short, the problem is too much data, 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.
- Session or packet 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. 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 Visibility and Analytics Fabric™ (VAF), as well as obtain additional key application metadata elements. Gigamon’s patented 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 VAF establishes a scalable framework to deliver pervasive, flow-level visibility across networks and datacenters 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

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pervasive visibility with NetFlow generation across the entire network</td>
<td>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</td>
</tr>
<tr>
<td>High-throughput out-of-band NetFlow solution</td>
<td>No performance impact of NetFlow generation on production routers and switches</td>
</tr>
<tr>
<td>Unsampled 1:1 NetFlow generation on every packet</td>
<td>Complete and precise picture of network activity for security monitoring without loss of fidelity incurred from sampled NetFlow generation</td>
</tr>
<tr>
<td>Support for a wide range of NetFlow export formats – v5, v9, IPFIX, and CEF</td>
<td>Compatibility with legacy and next-generation NetFlow collectors</td>
</tr>
<tr>
<td>Ingress filtering on Layer 2, Layer 3, and Layer 4 headers using Gigamon Flow Mapping</td>
<td>Generate flow statistics for specific networks and applications</td>
</tr>
<tr>
<td>Support for up to six collectors with customizable templates and filters</td>
<td>Leveraging multiple vendors for security and application monitoring</td>
</tr>
</tbody>
</table>

# Key Metadata Extensions

<table>
<thead>
<tr>
<th>Extension</th>
<th>Fields Extracted</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>dnsIdentifier, dnsOpCode, dnsResponseCode, dnsQueryName, dnsResponseName, dnsResponseTTL, dnsResponseIPv4Addr, dnsResponseIPv6Addr</td>
<td>Uncover domain lookups for malicious command and control (C&amp;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</td>
</tr>
<tr>
<td>URL</td>
<td>URL from method types: HTTP GET, POST, PUT, DELETE, HEAD</td>
<td>Identify malicious communications to C&amp;C servers, Identify potential SQL and other OWASP vulnerabilities from URLs, Identify productivity and compliance violations using URL metadata</td>
</tr>
<tr>
<td>HTTP Response Codes</td>
<td>HTTP Response Codes: 100–199 (informational), 200–299 (success related), 300–399 (redirection), 400–499 (client requests), 500–599 (server related)</td>
<td>Baseline of HTTP codes to uncover anomalous behavior patterns, Identify excessive redirects (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&amp;C servers from infected hosts</td>
</tr>
</tbody>
</table>
### Key Metadata Extensions, continued

<table>
<thead>
<tr>
<th>Extension</th>
<th>Fields Extracted</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| Certificates | • sslCertificateSubject  
• sslCertificateValidNotBefore  
• sslCertificateValidNotAfter  
• sslCertificateSerialNumber  
• 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 Cloud Suite for processing in public or private cloud environments, and 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.

**About Gigamon**

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon Hawk Cloud Visibility and Analytics Fabric delivers advanced intelligence so that security, network, and application performance management solutions in enterprise, government, and service provider networks operate more efficiently. As data volumes and network speeds grow and threats become more sophisticated, tools are increasingly overburdened. One hundred percent visibility is imperative. Gigamon is installed in more than three-quarters of the Fortune 100, more than half of the Fortune 500, and nine of the ten largest service providers.

For more information about Gigamon Hawk visit: [gigamon.com](http://gigamon.com)