Application Note

NetFlow Generation

Introduction

NetFlow is a network protocol originally developed by Cisco Systems to collect statistics on IP traffic information. NetFlow has since been adopted as an ITEF standard (RFCs 3954 and 5101) and is broadly used for traffic monitoring. Using NetFlow, devices like routers and switches gather and forward metrics to one or more monitoring stations. NetFlow is a simple, effective way to increase visibility of the traffic types and usage patterns across systems. Understanding network usage is critical not only for optimizing network performance, business systems, and quality of service, but also for catching denial of service attacks, data extraction, and other events that represent a security risk. The statistics-based NetFlow information complements traditional packet-based analysis, and by combining the two into a single Unified Visibility Fabric™ architecture, Gigamon® provides network administrators, security officers, and application owners with a comprehensive view of network activity and performance.

Key Customer Applications

NetFlow statistics are used in the following ways:

- **Network Monitoring:** Utilize flow-based analysis techniques to visualize traffic patterns associated on a network-wide basis
- **Application Monitoring and Profiling:** Obtain a statistical, time-based view of application usage over the network
- **User Monitoring and Profiling:** Gain basic understanding of customer/user utilization of network and application resources which may be used to detect and resolve potential security and policy violations
- **Network Planning:** Track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, or higher-bandwidth interfaces
- **Security Analysis:** Detect changes in network behavior to identify anomalies that are clearly demonstrated in NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents
- **Accounting/Billing:** Provides metering for resource utilization accounting

Existing Solutions

NetFlow Generation is typically undertaken by the routers and switches as part of the production network. Enabling NetFlow Generation on a device is a simple configuration change where you specify the destination that will act as the flow receiver (or collector). However NetFlow does have a performance impact on the devices where it is implemented. The processor and memory load can cause severe service degradation on the network devices, normally measured as an increase in the device CPU and memory utilization in order to track and report on these conversations. Separate, standalone devices may also be used to generate NetFlow statistics; however this tends to be a costly solution if the device provides no other value.

Disadvantages

Below is a brief summary of the disadvantages of using the production network to generate NetFlow.

1. Performance taxes the routers and switches processing statistics when generating NetFlow information. It may affect the device's ability to pass traffic without introducing latency and packet drops.
2. Due to the potential risk of dropping production traffic as a result of NetFlow Generation, networking devices often resort to sampling packets to generate statistics. A low sampling rate (sometimes as low as 1 in 1000 packets) can result in missing out on important events that are happening in the network.
3. Routers, switches, and firewalls do not always support NetFlow Generation. Some use other proprietary protocols of their own.

4. Monitoring tools and NetFlow collectors are expected to support multiple versions of NetFlow which in some cases can be custom vendor-specific versions.
5. NetFlow records can only be forwarded to a limited number of collectors or monitoring tools; this number can be far fewer than required to properly manage and troubleshoot the network.
6. Very limited ingress and egress filtering capabilities severely limits the ability to pick the flows of interest to generate NetFlow.

Gigamon Solution

Given that Gigamon's Visibility Fabric™ has access to all the traffic that is flowing through the network, GigaVUE® fabric nodes are in a unique position to not only generate NetFlow statistics, but also provide visibility into normal traffic operations. Using this out-of-band approach eliminates any risk to the production network.

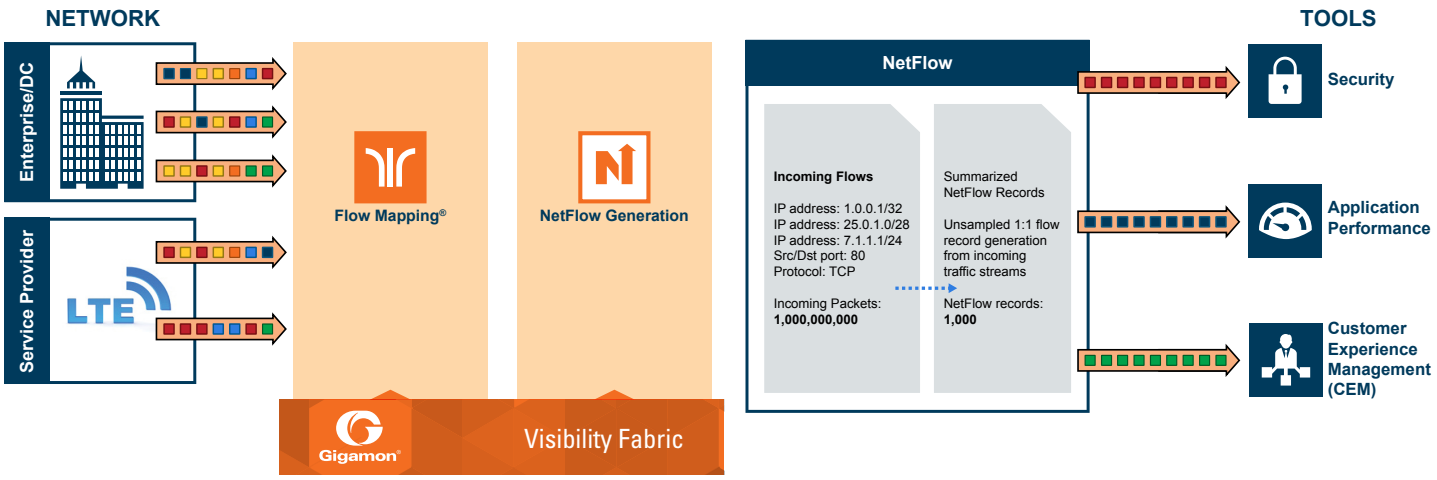

Figure 1: NetFlow Generation

Enhanced flow-level visibility can be used for deriving information around usage patterns, capacity planning, top talkers, and applications. However, flow-based data is summarized information and does not provide access to a specific set of packets. Not having this information can also severely impede detailed analysis around latency/jitter, application performance, customer experience, security threats, etc. Gigamon's Visibility Fabric architecture is the first in the industry to provide NetFlow-based flow statistics in parallel with the raw packet streams, enabling users to monitor, troubleshoot, and optimize their networks.

Leveraging the processing capabilities enabled with GigaSMART® technology, users can generate NetFlow statistics at higher sampling rates or even at line-rate, which enables much more accurate analytics. Enhanced flow-level visibility can be used for deriving information around usage patterns, capacity planning, top talkers, and applications, and building relationships between network elements.

Key Features

- First in the Industry to Combine End-to-End Traffic and Flow Visibility in a Single Solution
  - High-throughput solution with support for unsampled 1:1 NetFlow record generation
  - Integrated traffic visibility solution with NetFlow Generation
- Out-of-Band NetFlow Generation
  - Transforms packet data across multiple devices into summarized NetFlow statistics
- Supported NetFlow Export Formats
  - v5
  - v9
  - IPFIX

- Ingress Filtering
  - Leveraging Gigamon's patented Flow Mapping® technology, pick and choose incoming flows based on Layer 2, Layer 3 or Layer 4 header parameters to generate NetFlow information
- Export Filters
  - Advanced filters for custom exports to one or multiple NetFlow collectors, performance and security monitors
- URL Collection (IPFIX only)
  - HTTP: GET, POST, PUT, DELETE, and HEAD method types
  - HTTP response codes (2XX,3XX,4XX..) to help uncover suspicious behavior such as redirects and DOS attacks
  - SIP: INVITE, ACK, BYE, REGISTER, OPTIONS, and CANCEL request types
- Multiple NetFlow Exports
  - Supports NetFlow exports to up to six (6) NetFlow collectors; most switches and routers support limited numbers of collectors
  - Filter output for specific collectors or replicate output across multiple collectors
- Combining End-to-End Traffic and Flow Visibility
  - Integrated traffic visibility solution combining Gigamon's patented Flow Mapping technology-based traffic distribution with GigaSMART capabilities and NetFlow Generation

Key Benefits

- Optimize Production Network
  - Offload NetFlow Generation to the Visibility Fabric to avoid expending expensive production network resources
- Minimize Risk to Production Networks
  - Out-of-Band Solution completely eliminates the risk of losing production traffic as a result of generating NetFlow statistics
- Facilitate Big Data Analytics
  - Increased visibility in to traffic types and usage patterns across Big Data environments
- Improved Monitoring and Security
  - Unsampled flow data provides a complete and precise picture of network activity
- Enhance Remote Monitoring
  - Summarized NetFlow statistics across remote sites
  - Optional drill-downs in to raw packet analytics for detailed trouble-shooting and root-cause analysis
- Optimize Operational Efficiency
  - Gain comprehensive network visibility from multiple network observation points
  - Custom NetFlow exports to meet specific management needs
- Facilitate Network Security Enforcement
  - Enable full network protection with visibility into every flow
- Standardize on NetFlow Versions
  - Facilitate enterprises and service providers to standardize on a specific NetFlow version across their entire monitoring infrastructure
  - Eliminate the burden of supporting vendor specific custom versions of NetFlow for monitoring tool vendors

Summary

NetFlow is a key component of a complete monitoring solution, providing vital input to a variety of statistical tools. The primary NetFlow drawback is the fundamental processing requirements needed to generate the metrics. This can impact the performance of the switch or router, potentially causing packet drops. By offloading this processing to GigaVUE fabric nodes, basic IT infrastructure risk is removed. NetFlow Generation is just one of the many benefits that can be derived from the Gigamon Unified Visibility Fabric™ architecture.

About Gigamon

Gigamon provides an intelligent Unified Visibility Fabric™ to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and dozens of government and state and local agencies.

For more information about the Gigamon Visibility Fabric architecture visit: **www.gigamon.com**

4027-04 11/15

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