Packet and Advanced Flow Slicing

The Challenge of Irrelevant Data

In an organization's operations center, their network performance monitoring (NPM), customer experience management (CEM) and out-of-band (OOB) security tools are all too often overloaded with traffic that they need to analyze. In response, the organization may use a network packet broker (NPB), which may use rudimentary Layer 2 to 4 filtering rules to reduce the amount of traffic sent to the tools, but this frequently still leaves too much volume for a single tool to handle. The NPB can also apply load-balancing to spread the sessions across multiple instances of a single tool type, but this requires multiple instances of the same tool. This increases the cost of the monitoring solution.

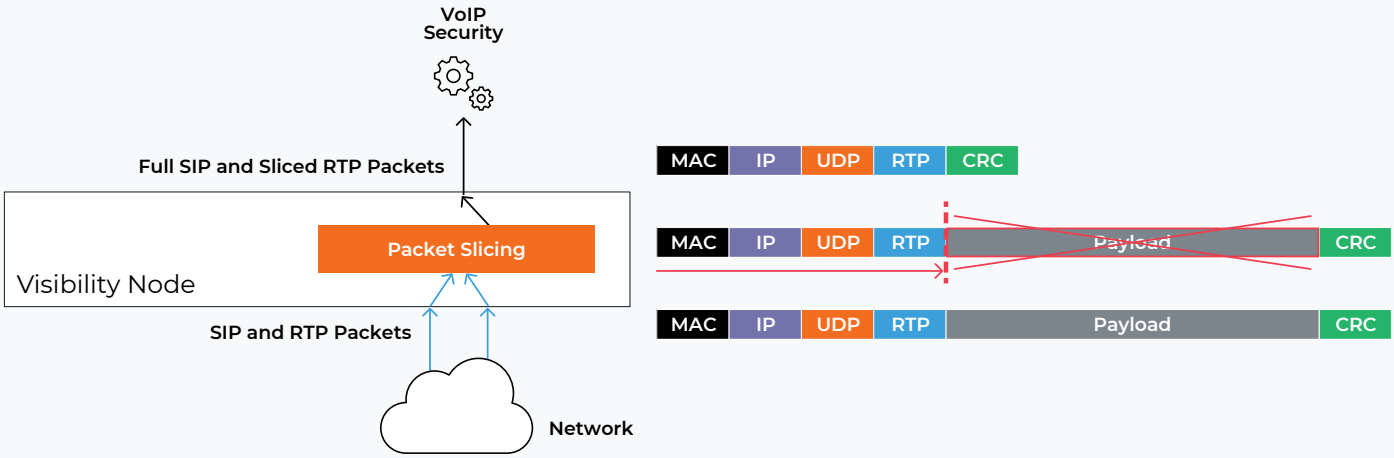

Figure 1. A visibility node slicing off unnecessary payload from packets.

Key Benefits: Optimize the Tool Infrastructure

- Optimize tools' processing by forwarding only useful packet and flow information
- Improve packet and flow capacity into the tools
- Improve ROI from tool infrastructure

In addition, the tools themselves may not need to see very deep into the packets or flows to perform their analysis, since only the leading headers in the packets, even up to Layer 7, are necessary. So, by flooding each tool instance with all the needed traffic packets and flows, but with all the unnecessary content, the efficiency of the tools is dramatically reduced.

Truncating the Content

There is, however, an effective solution. Gigamon offers two methods of truncating packets and flows that typically achieve between 60–90 percent reduction in traffic volume sent to a specific tool, thereby enabling the tool to be far more efficient by processing more packets and flows and reducing the need to spread the load across multiple instances of the same tool.

#1. Gigamon Packet Slicing

The first is Packet Slicing, which lets you remove all payloads from select packets starting from a specific location in the packet. The procedure performed is as follows:

- On a packet-by-packet basis, each packet is evaluated to determine if it is to be sliced, based on user-specified filtering rules
- Once selected, the location is found in the packet for where the slicing will start, based on user-specified location criteria
- Then, the remainder of the packet is removed, the Ethernet frame CRC/FCS is recalculated and the new CRC/FCS is added to the end of the packet

The example in Figure 1 shows the removal of the media payload contained in real-time transport protocol (RTP) to be forwarded to a VoIP Security tool that analyzes information only in the Layers 2 to 4 and RTP headers. The SIP packets remain intact, since the tool needs to see the entire SIP payload. In such an example, you can reduce VoIP traffic volume by roughly 80 percent.

#2. Gigamon Advanced Flow Slicing

The second solution is Advanced Flow Slicing. After a specific number of initial packets in a flow, all subsequent packets in the flow are either dropped or have all payload removed.

The procedure performed is as follows:

- On a flow-by-flow basis, each flow is evaluated to determine if it is to be sliced, based on user-specified filtering rules
- Once selected, the user-defined number of packets is allowed through intact, and then, based on user configuration, all subsequent packets in the flow are either:
  - Dropped, or
  - Sliced as per Packet Slicing described above.

Figure 2 shows an example of truncating the packets in HTTPS flows to be forwarded to a CEM tool that is unable to decrypt the payload and unable to analyze it in encrypted form. The HTTP packets remain intact, since the tool can analyze the unencrypted payload. In such an example, you can reduce total HTTP/HTTPS traffic volume by least 60 percent.

With Gigamon Packet Slicing and Advanced Flow Slicing applications, network operations can dramatically improve the efficiency of their existing and new monitoring tools.

You can combine Packet Slicing and Advanced Flow Slicing with other GigaSMART® intelligence applications, such as those within the Traffic Intelligence, Application Intelligence and Subscriber Intelligence, which enables monitoring tools to perform as effectively and efficiently as possible.

Pervasive Deep Observability

In this era of big data, network operations and information security have searched for a way to efficiently and effectively monitor performance and security for their subscribers.

Gigamon allows convergence on a single deep obervability pipeline that not only simplifies and automates network traffic visibility, but also provides built-in intelligence to address big data. This can shape how operations chooses to monitor and manage its networks to run fast and stay secure.

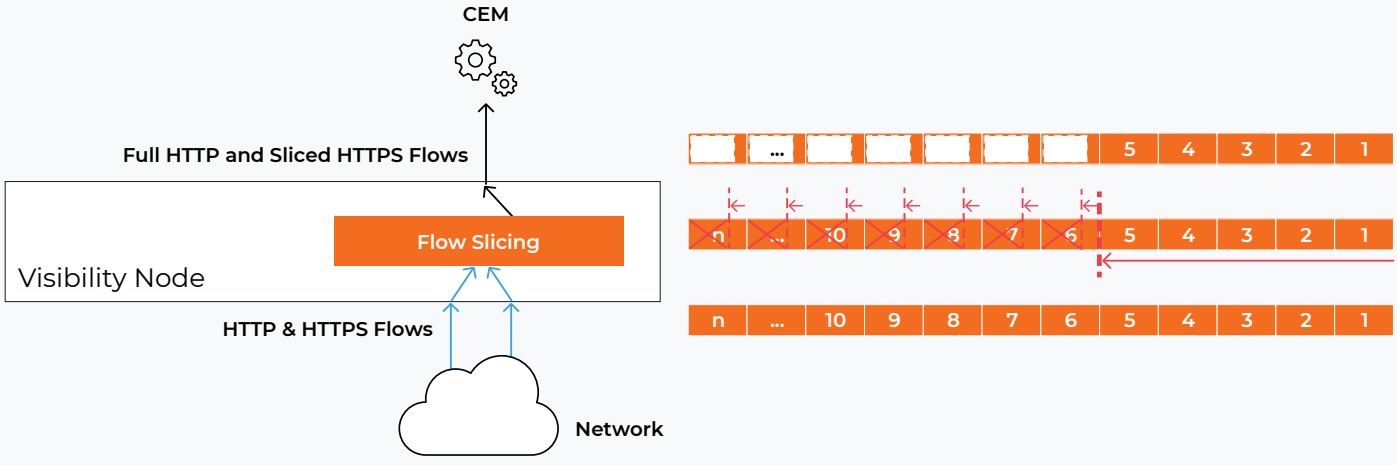

Figure 2. A visibility node slicing off unnecessary payload from only trailing packets in a flow.

Legacy approaches to monitoring have offered limited traffic visibility with limited traffic and data reduction capabilities. They are difficult and costly to scale and manage, and often require change orders or network downtime to adapt to an evolving network.

The Gigamon Deep Observability Pipeline, in contrast, provides the architecture and intelligence for network operations and information security teams to create a monitoring infrastructure designed for the era of big data and delivers pervasive visibility, awareness and control from the converged edge to the cloud. Sitting between the IT infrastructure and the tools that need the access to data, the Gigamon Deep Observability Pipeline provides a holistic approach to traffic visibility that includes:

- **Architecture advantages:** The GigaVUE® family of visibility nodes offers the volume, port density and scale needed to connect the right analytical tools to the appropriate large or bonded pipes. Tool trials are streamlined, new tools can easily be added or removed, and uptime is protected while downtime is prevented with a solution that is outside the production network and provides pervasive visibility.
- **Feature advantages:** Advanced filtering, packet manipulation and session-aware traffic identification reduce the amount of data arriving at each tool, while ensuring that the data is formatted precisely for the tool's consumption. Because each tool doesn't need to parse the incoming stream or waste processor cycles on nonrelevant data, it can be optimized and focused on the more important task of data analysis.
- **GigaSMART applications:** Traffic Intelligence, Application Intelligence and Subscriber Intelligence provide effective monitoring of large-to-massive traffic volumes through the logical reduction of traffic, which is more suitable for connecting to existing tools with lower speed ports or limited capacity. Gigamon Packet Slicing and Advanced Flow Slicing applications enable more cost-effective and efficient traffic obervability.

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/support-and-services.html.

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, nine 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

04.23_02