ACCELERATED PCAP: AN ARCHITECTURE FOR PRECISION PACKET CAPTURE AND ANALYSIS ON HIGH-SPEED NETWORKS
CONTENTS

Background and Objectives ........................................... 3
Value to Enterprise ....................................................... 3
Line-Rate Capture and Replay ......................................... 3
Precision Time Stamping ................................................. 3
Intelligent Data Flow ...................................................... 3
Technical Approach ....................................................... 4
Conventional PCAP ....................................................... 4
Accelerated PCAP Architecture ......................................... 5
BACKGROUND AND OBJECTIVES
There are a number of tools and capabilities available to engineers and administrators to help them manage and secure large and small-scale networks alike. Still, few capabilities are as fundamental to this task as packet capture (PCAP). A mechanism for intercepting data packets that are traversing a computer network, PCAP is a common capability deployed within an organization to monitor for security events, identify data leaks, monitor network performance, troubleshoot issues, and even to perform forensic analysis to determine the impact of network breaches.

Effective PCAP and analysis systems can provide administrators and engineers with an accurate, real-time view of what is happening within a network infrastructure. Likewise, precision PCAP systems can provide organizations with the ability to re-create network events with high fidelity for verification and validation of architectural changes, troubleshooting and even forensic analysis. As network speeds continue to increase, existing PCAP systems are struggling to keep up with the demands of performing precision capture and replay at 1/10/40/100 Gbps speeds.

This paper will illustrate how the use of acceleration technology from Napatech, coupled with open source network monitoring and capture solutions, can enable organizations to keep up with the demands of precision packet capture and replay on high-speed networks.

VALUE TO ENTERPRISE
The use of FPGA (Field Programmable Gate Array) based network acceleration technology from Napatech can immediately improve on organization’s ability to monitor and react to events that occur within its network infrastructure. The coupling of open source tools with the speed and accuracy of programmable logic provides:

LINE-RATE CAPTURE AND REPLAY
Napatech’s FPGA-based network acceleration cards (NACs) are ideal for performing high-speed packet capture and replay at 1/10/40/100 Gbps speeds. Moreover, Napatech acceleration cards allow for precise inter-frame gap (IFG) control, which is critical when replaying captured traffic for troubleshooting or simulation of traffic flows.

PRECISION TIME STAMPING
Napatech NACs provide hardware-based high-precision time stamping with nanosecond resolution for every frame captured and transmitted. Hardware-based time stamping avoids the unpredictable latency inherent in software-based solutions and enables a communication flow to be recorded precisely as it occurs. Precision time protocol (PTP) is also supported for accurate synchronization across distributed network probes.

INTELLIGENT DATA FLOW
To maintain capture and analysis performance at high speeds it is important to identify and direct traffic flows immediately upon ingress to minimize the load on user-space applications. Napatech NACs provide the ability to dynamically identify and direct data flows into specific CPU cores based on the type of traffic being analyzed.

TECHNICAL APPROACH
CONVENTIONAL PCAP
Historically, organizations have relied on software tools to perform packet capture and analysis on their network infrastructure. In this case, software is installed on a designated monitoring host and configured to poll packets from a commodity network adapter placed in promiscuous mode and connected to the network via a SPAN interface. A typical architecture for low-speed PCAP using a commodity NIC and libpcap is illustrated in Figure 1.
In this scenario, each time the network adapter receives an Ethernet frame, it generates an interrupt request and copies the data from the memory buffer on the adapter into kernel space. Normally, the kernel space driver would determine if the packet is intended for this host and either drop the packet or pass it up the protocol stack until it reaches the user-space application it is destined for. However, when configured for promiscuous mode, all packets are captured in a kernel buffer regardless of destination host. Once the kernel buffer is full, a context switch is performed to transfer data to a user-space buffer managed by libpcap so that the data can be accessed by user level applications. This intermediate buffer remains hidden to user level applications and is necessary to prevent applications from accessing kernel-managed memory.

Given this architecture, it is clear that some amount of time will lapse between when a frame is received by the adapter and actually delivered to the user-space application for processing. At low data rates this lapse in time does little to affect PCAP accuracy, but at higher rates this latency is compounded and CPUs become saturated trying to keep pace with incoming data leading to capture loss and timing issues.

Consider, for example, that a 1 Gbps network link can push around 1.5 million packets per second, or one packet every 670 nanoseconds. Conversely, at 10 and 100 Gbps speeds systems are processing one packet every 67 or 6.7 nanoseconds respectively. Simply capturing traffic at this rate in a conventional architecture is enough of a challenge without the added complexity of precise timing, categorization, flow identification and filtering. Performing lossless, high fidelity packet capture, replay and real-time analysis of data flows at these rates requires a different approach to PCAP, one that moves the bulk of the data processing out of the user-space and into the hardware while also eliminating the inefficiency of user to kernel space interactions.

**ACCELERATED PCAP ARCHITECTURE**

Achieving the goals of PCAP on high-speed networks is possible with a hardware-accelerated approach. The targeted use of programmable logic coupled with open source tools allows data to be accurately captured and processed within the NAC before it is passed into user-space applications. Figure 2 illustrates what an accelerated PCAP architecture might look like.

Napatech NACs use programmable logic, FPGAs, to perform in-line event processing and line rate packet analysis in hardware at 1/10/40 Gbps speeds. In an accelerated PCAP architecture, this capability is leveraged to push most of the frame processing into the hardware of the capture device, which can be deployed within a commodity server or workstation, preserving CPU cycles for higher-level analysis.
This approach ensures that by the time data is passed to the user-space buffer for access by applications it has already been time stamped, categorized and filtered appropriately.

By coupling these devices with open source applications, powerful – yet cost effective – solutions can be built for a variety of purposes. Napatech NACs support industry standard PCAP applications, such as:

- WireShark
- tcpdump
- tcpreplay
- Suricata
- SNORT
- Ostinato
- Bro

In general, Napatech NACs enable easy in-house development of scalable, high-performance network applications over PCAP. Even complex payload analysis and network-wide correlation algorithms can be easily scaled by the effective flow-based load-balancing mechanism built-in to the NAC. And the more complex analysis that the application performs, the more critical it is that the PCAP stream from the capture device has no packet drops and the frames are in the correct order. Tasks like protocol reconstruction, reassembly, event detection, and quality of service (QoS) calculations are severely impacted by insufficient PCAP performance.

In addition to the performance benefits, an extremely important element of the accelerated PCAP architecture is the ability to establish the precise time when frames have been captured. At 10 and 100 Gbps speeds an Ethernet frame can be received every 67 or 6.7 nanoseconds respectively. This makes time stamping at the nanosecond level essential for uniquely identifying when a frame is received.

Napatech acceleration cards provide the ability to perform high-precision time stamping with nanosecond resolution on every frame captured or transmitted. Similarly, support for IEEE 1588, or Precision Time Protocol (PTP), allows Napatech NACs to maintain precise time synchronization in a distributed deployment where multiple accelerated PCAP probes are deployed throughout a network infrastructure. This allows frames to be merged from multiple ports on multiple cards into a single, time-ordered analysis stream. Maintaining this level of temporal fidelity within the capture ensures that organizations can perform retrospective analysis of network events by replaying data in exactly the same way as it was captured, complete with precise timing and inter-frame gap control.
Providing a real-time view of what is happening within a network, as well as the ability to perform a retrospective review of activity, is critical to understanding and measuring performance, identifying bottlenecks, troubleshooting issues and securing the environment. As such, packet capture and analysis continues to play a critical role in managing and securing large and small-scale networks. However, traditional means of performing PCAP are being out-paced by today’s high-speed network fabrics, leading to large amounts of dropped packet data and imprecise collections. Enabling PCAP at 10/40/100 Gbps speeds and beyond necessitates that the processing of captured packets be pushed to the point of ingest, leveraging hardware acceleration to maintain precise, lossless capture at these speeds. Using programmable logic and open source software deployed on commodity servers, a novel architecture can be conceived that can meet the demands of PCAP on high-speed networks for years to come.

**COMPANY PROFILE**

Napatech is the world leader in accelerating network management and security applications. As data volume and complexity grow, the performance of these applications needs to stay ahead of the speed of networks in order to do their jobs. We make this possible, for even the most demanding financial, telecom, corporate and government networks.

Now and in the future, we enable our customers’ applications to run faster than the networks they need to manage and protect.

_Napatech. FASTER THAN THE FUTURE_
Enabling PCAP at 10/40/100 Gbps speeds and beyond necessitates that the processing of captured packets be pushed to the point of ingest, leveraging hardware acceleration to maintain precise, lossless capture at these speeds.
EUROPE, MIDDLE EAST AND AFRICA
Napatech A/S
Copenhagen, Denmark
Tel. +45 4596 1500
ntemeasales@napatech.com
www.napatech.com

NORTH AMERICA
Napatech Inc.
Boston, Massachusetts
Mountain View, California
Washington D.C.
Tel. +1 888 318 8288
ntamericassales@napatech.com
www.napatech.com

SOUTH AMERICA
Napatech Brasil Ltda.
São Paulo, Brazil
Tel. +55 11 2127 0782
ntsouthamericasales@napatech.com
www.napatech.com

APAC
Napatech Japan K.K.
Tokyo, Japan
Tel. +81 3 5326 3374
Napatech Korea
Seoul, South Korea
Tel. +82 2 6001 3545
ntapacsales@napatech.com
www.napatech.com