

# The Depths of Netronome Deep Packet Inspection

## THE NEED FOR DEEP PACKET INSPECTION (DPI)

In a short time, network infrastructure bandwidth has scaled exponentially to 10Gbps with designs for the next generation of Ethernet promising between 40Gbps to 100Gbps. At the same time, the complexity and breadth of applications that run over these backbones are drastically changing. Accordingly, to accommodate the ever-increasing need for network security, control and visibility that is required for network traffic, communications equipment needs to be protocol-, content- and application-aware at increasingly higher and higher speeds.

## DPI DEFINED

DPI is the ability to analyze and understand network traffic at L2-L7 for security, service assurance, quality of service (QoS) and application rate-limiting. DPI provides more extensive and detailed flow awareness to network applications than simple L2-L4 classification by examining the packet contents, as well as the packet headers. DPI also provides network administrators with the ability to examine traffic at all network layers across a series of datagrams giving insight into the source, destination, application and intent of the traffic in question. In contrast to DPI, traditional classification only provides L2-L4 header analysis and is not a dependable mechanism to determine protocol and application; nor is it an adequate technique to analyze specific application-level details within a flow between a set of hosts. Many protocols do not use standard IP protocol values, or use non-standard and negotiated TCP/UDP port numbers for connection establishment. Application and protocol identification is often buried further in the packet, or is spread across several packets in the transaction, making individual packet header analysis ineffective.

This need for increasing content awareness applies not only to fixed LAN/WAN-based networks, but increasingly to mobile networks, as well. With the bandwidths that 3G wireless and LTE networks offer (up to 100Mbps downloads), along with the converged data, voice and video services that users will utilize over these networks, we can expect wireless networks to support all of the same services as fixed networks and share vulnerabilities to the same types of threats.

## DPI AND PLATFORM CHALLENGES

To satisfy the needs of network operators for DPI-based solutions, the platforms on which these applications are hosted share a common set of requirements. DPI implementations must:

- Support traditional analysis of common L2-L4 packet header fields, including source and destination IP address, IP protocol, source and destination TCP/UDP port numbers, DiffServ Codepoint (DSCP) and ingress interface/VLAN;
- Support analysis of all network protocol layers and full packet payload/content;
- Support identification of applications with static, dynamic and negotiated protocol and port fields;
- Be able to interrogate multiple packets during connection establishment extending beyond the standard TCP handshake (SYN, SYN-ACK, ACK);

NETRONOME  
WHITE PAPER

## OVERVIEW

*Netronome envisions an evolution in communications networks where every link between clients, infrastructure and servers is high-performing, intelligent and secure. A combination of increasing bandwidth, greater security requirements and the need for application and content-aware networking are driving the evolution to intelligent networking (L2-L7) from today's simpler (L2-L3 only) networks.*

*For designers of communications equipment whose network processing requirements extend beyond simple forwarding, Netronome's Network Flow Processors (NFPs) deliver high-performance packet processing with intelligence, security and virtualization for millions of simultaneous flows, making them ideal for deep packet inspection (DPI) applications. Unlike network processors and multicore CPUs that lack L4-L7 programmability or cannot scale to 10Gbps and beyond, Netronome's NFPs are powered by 40 programmable networking cores that deliver 2000 instructions and 50 flow operations per packet at 30 million packets per second (pps), enabling 20Gbps of L2-L7 processing with line-rate security and I/O virtualization.*

NETRONOME™

*Intelligent to the Core.™*

netronome.com

- Support a signature database for identification of common applications;
- Be completely flexible and programmable in order to handle the ever-changing and evolving set of protocols, applications, services and threats;
- Provide full analysis at line rates, if only a portion of data can be deeply inspected without loss, the inspection process provides little value;
- Support inline (active) and offline (passive) configurations; and
- Support the ability to take a varied set of actions based on packet and flow analysis, including:
  - Active and passive packet dropping
  - Marking or tagging of traffic
  - Content Insertion
  - Queuing/policing/shaping/rate limiting of flows
  - Redirection
  - Load Balancing
  - Counting/metering/statistics gathering and analysis

### A NEW DPI ARCHITECTURE IS NEEDED

In order to achieve these combined DPI requirements, along with the increasing need for network I/O virtualization, a high-performance flow processing architecture is necessary. This is best achieved through a heterogeneous processing architecture combining virtualized I/O network-coprocessing with multicore x86 general-purpose CPUs. Neutronome's high-performance Network Flow Processors (NFPs) are specifically designed for use in this heterogeneous architecture. The highly programmable, 40-core NFP with integrated cryptography supports tight coupling with general-purpose multicore CPUs, enabling equipment providers to quickly deliver high-performance networking and security products. In addition, source-code compatibility with the market-leading IXP28XX processors enables investment protection for existing field-proven networking algorithms, while speeding time-to-market for new-generation products at the lowest development cost and risk.

### COMPETITIVE APPROACHES

Traditional network and communication processors are not adequate to meet these extensive and challenging L2-L7 requirements at such sustained line speeds. Other processing solutions, such as multicore MIPS architectures, are capable of DPI, though with performance penalties. These architectures require that all packet processing occurs in general-purpose processors, but lack integrated security and the required data plane interconnect throughput for communication with higher-speed multicore processors or look-aside packet processing hardware. As network speeds increase, the multicore MIPS model does not scale in situations where every packet of every flow needs DPI. An alternative processing solution, fixed-function network processors, may operate at high data rates, but these devices provide neither the programming flexibility to run DPI algorithms in hardware nor the ability to parse data beyond L2-L4 headers.

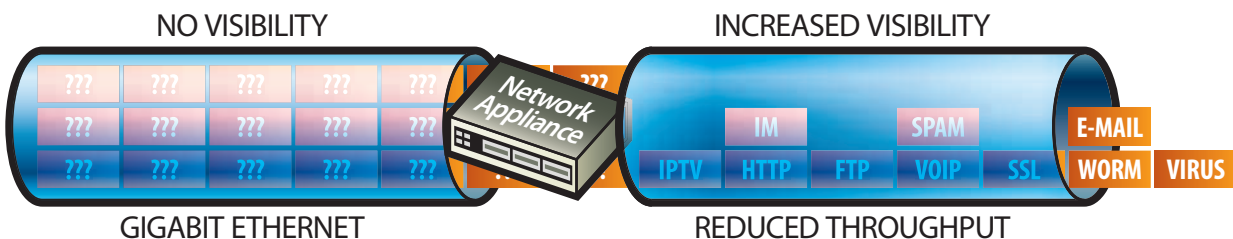
### GRANULAR FLOW ANALYSIS WITH DEEP PACKET INSPECTION

Neutronome provides a full suite of solutions intended for DPI applications requiring detailed and accurate analysis of network traffic at increasing data rates. These solutions range from high-performance, highly programmable network flow processors to acceleration cards based on this silicon.



This hardware is coupled with software modules/blocks designed to leverage the intelligence and speed of these flow processors specifically tailored for DPI.

Today, Neutronome customers have access to DPI capability built on the Neutronome Flow Engine (NFE), which uses the Intel® IXP28XX network processor, and Neutronome's Flow Management (NFM) software suite that exposes the DPI abilities of the IXP via simple application programming interfaces (APIs). These APIs provide developers with an abstraction layer that hides packet processing occurring in hardware-based microengines. Together, the NFE and NFM allow a developer to easily identify applications and protocols based on patterns and behavior analyzed deep within a flow. The current release of NFM allows a user to classify, detect and act upon specific protocols and applications.



*Network appliances have failed to keep pace with improvements in network performance.*

NFM provides a full suite of L2-L7 flow analysis and deep packet inspection capabilities, including:

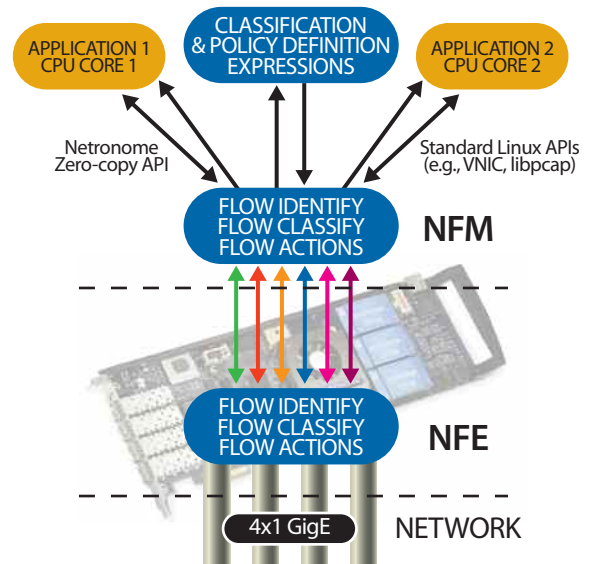
- Classification of flows based on values of well-known packet header fields of Ethernet (including 802.1p/q) and IP;
- Identification of applications and protocols with fixed or well-known TCP/UDP ports or IP types;
- HTTP 1.0/1.1, including embedded transactions and chunked encoding;
- E-mail protocols, including POP3, SMTP and IMAP;
- Additional protocols embedded in HTTP, such as SOAP and Web conferencing;
- Associated media and data flows, including FTP and SIP;
- VoIP, IPTV and other streaming media, such as SIP, RTP and VLC;
- IP Tunnels, including GRE, L2TP, PPTP, IPsec, IP in UDP or TCP; and
- Common peer-to-peer (P2P) applications, such as BitTorrent, Gnutella, FastTrack, Jabber and WinMX.

NFM allows active (inline) or passive (offline) enterprise and networking applications to perform one or more unique actions on flows once they have been identified, including:

- “Cut-through” – All classified flows are switched through the appliance in hardware by the NPU.
- “Load balancing” – Flows can be load-balanced across CPU cores for added application performance.
- “Redirection” – All classified flows are diverted to the CPU for processing by the host application.
- “Tee” – All approved flows are cut-through the appliance. Additionally, select classified flows are copied to the CPU where further processing can be performed by the host application.
- Tunnel Mode, where IP tunnels (e.g., GRE) can be terminated and re-originated, enabling the creation of virtual overlay networks; and
- Statistics and Monitoring mode, where the NFM is used to gather detailed packet and flow-level statistics and perform general application and flow monitoring.

As NFM classifies a protocol, specific pre-defined fields of that protocol are identified and exposed to the user in an easy-to-comprehend format. For example, when HTTP is classified, the user has access to fields within the protocol, such as the HTTP request header fields, request URL, request content type and much more. Classifying the protocol and segmenting the data into well known fields saves development time and provides an easier DPI model to work with, unlike other DPI solutions that simply provide a pointer to a packet which forces the developer to locate and interpret the fields of interest for each supported application.

Identifying an application is not the only function of DPI and the Netronome toolset. Based on the DPI analysis, the NFM also has the ability to apply actions to flows (classified by the 5-tuple within an application session), rather than to single



packets, offering powerful, stateful flow analysis to applications. Once an application has been identified, the NFM and IXP break down the flow data into fields which represent the segments that make up the protocol or application. Dissecting and presenting flows in this manner allows developers to easily understand and analyze the protocols which require inspection. Once DPI is complete on a portion of a flow, actions, such as flow termination, fast-path/cut-through, rate limiting, guaranteed QoS and others, can be implemented on subsequent packets of that flow.

Netronome will continue to add capabilities to our DPI software for new and emerging protocols and applications; and will make an extensive development toolset available to customers to expand their own custom DPI capabilities. Specifically, support for P2P applications, like Skype and eMule, and popular instant messaging applications, such as MSN, Yahoo Messenger and AIM, are immediate targets.

## DPI WITH NFP-3200

As part of the next-generation NFP-32XX line of network flow processors, Netronome intends to extend the DPI capability available in today's NFE cards and IXP processors by coupling a high-performance intelligent data plane based on programmable microengine (ME) cores and the required tools to allow users to easily design and develop their own DPI solutions. Because these ME cores contain instruction sets optimized around high-performance packet processing, detailed packet and flow inspection can be performed on greater levels of traffic without compromising security or performance. The Netronome NFP-32XX supports 40 ME cores operating at 1.4Ghz, each with 8 threads. This provides the ability to perform almost 2,000 operations per packet on 10GigE line-rate traffic for minimum-sized datagrams (64 bytes). This unmatched speed and flexibility offers developers the ability to do far more than simple packet forwarding, but rather apply complex algorithms to both packet headers and content in hardware at line rate.

Depending on the nature of the application, most DPI functionality is implemented in NFP ME cores. At times, these powerful ME cores will be augmented by specialized hardware like tightly coupled general-purpose processors or regular expression hardware for pattern/signature matching to further extend expressiveness. The Netronome solutions, both the existing IXP-based NFE acceleration hardware and NFP-32XX-based products, are ideal in these types of heterogeneous processing environments. The IXP-based NFE cards support a PCIe x4 interface to multicore general-purpose processors and an extensive set of capabilities to load balance flows to these cores through zero-copy drivers. The NFP-32XX line of processors integrates the ARM11 core at 700MHz, a Gen-II PCIe 8-lane interface for high-speed communications with multicore x86 processors, virtualized I/O support and high-speed interconnects, including XAUI, SPI and Interlaken (ideal for interfacing with regular expression hardware).

The software components that complement the NFP-32XX are reusable pieces of code which can be used as development reference to reduce time-to-market or as complete blocks of software in finished DPI products. These blocks range from very small data or memory operations to complete functional blocks of code for complex packet processing tasks like header or content classification, load balancing, IP forwarding, Ethernet switching and TCP termination, to name a few.

## CONCLUSION

Netronome has extensive DPI research and development experience and numerous DPI deployments based on our existing IXP and IA designs. This intellectual property will be extended to our new NFP-3200-based network flow processors, NFP-based acceleration hardware and associated software components. Combining this experience with the performance and integration enhancements done on the NFP-3200, DPI applications can now become more intelligent in high-bandwidth environments.

**Daniel Proch can be reached at [daniel.proch@netronome.com](mailto:daniel.proch@netronome.com).  
Robert Truesdell can be reached at [truesdell@netronome.com](mailto:truesdell@netronome.com).**

## Deep Packet Inspection using NFP-3200

