

NETRONOME FLOW MANAGER

NETRONOME™

Acceleration for Network and Security Applications

To accommodate the complexity and breadth of applications and services that run over today's high-speed backbones, network appliances need to be increasingly protocol-, content- and application-aware at high speeds to achieve the combined requirements for network I/O, packet capture performance, deep packet inspection (DPI) and security processing. Existing solutions based on standard servers are not adequate to meet these L2-L7 packet processing requirements at such sustained line rates, and require specialized coprocessing. The Netronome Flow Manager (NFM), coupled with the Netronome's load balancing and acceleration hardware, enables application acceleration, DPI and flow analysis in a highly scalable manner for significantly increased application performance and greater control over network traffic.

NFM accelerates standard Linux® application programming interfaces (APIs) and provides an open API for development of network and security appliances and applications. NFM significantly reduces appliance CPU utilization and packet delay/jitter by offloading complex flow classification and packet processing to the Netronome Flow Engine (NFE). The NFM APIs provide developers with an abstraction layer that hides packet processing occurring in hardware-based micro-engines to allow users to benefit from acceleration while focusing development on their software applications.

The Netronome flow processing solution scales to 10Gbps, providing unmatched visibility and control of traffic at L2-L7 for over two million simultaneous flows, making NFM, tightly coupled with the Netronome load-balancing interface modules (LBIMs) and the NFE-i8000 acceleration hardware, an ideal solution for network appliances used for:

- Network security
- Intrusion detection and prevention (IDS/IPS)
- Policy enforcement/compliance
- Unified threat management (UTM)
- Deep packet inspection
- URL filtering and reverse proxying



- LAN/WAN bandwidth optimization
- Application load balancing
- Test, measurement and service assurance
- Lawful intercept (CALEA)

Granular Flow Analysis and Deep Packet Inspection

NFM allows simple identification of applications and protocols based on patterns and behavior through a full suite of L2-7 flow analysis and DPI capabilities. These include classification based on:

- Standard packet header fields, such as IP and Ethernet (including 802.1p/q)
- Identification of applications with fixed or well-known TCP/UDP ports or IP protocols
- HTTP 1.0/1.1 (with support for embedded transactions and chunked encoding)
- E-mail protocols, such as POP3, SMTP and IMAP
- 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
- Peer-to-peer applications, such as BitTorrent, Gnutella, FastTrack, Jabber and WinMX

APPLICATION

GET /generate_204 HTTP/1.1; User-Agent: Mozilla/5.0
Accept Encoding: gzip, deflate;
Accept-Charset: ISO-8859-1, utf-8

TRANSPORT

src port: 1286; dst port: 80; seq num: 1;
next seq num: 816; header length: 20 bytes

NETWORK

ip src: 10.0.0.10; ip dst: 64.233.161.100
protocol: TCP; version: 4;

DATA LINK

eth src: 00:19:b9:a3:42:44
eth dst: 00:15:58:7d:76:ed



Netronome's flow processors and network acceleration products offer a highly-programmable heterogeneous coprocessing environment that tightly couples the packet processing of the Netronome Flow Engine (NFE) microengine (ME) cores with the performance and ubiquity of general-purpose multicore systems. Netronome Flow manager (NFM) software allows appliance manufacturers to take advantage of this combination of ME cores and x86 platforms to quickly improve the performance of existing products and reduce overall development costs by accelerating the development of their network, security and DPI applications.

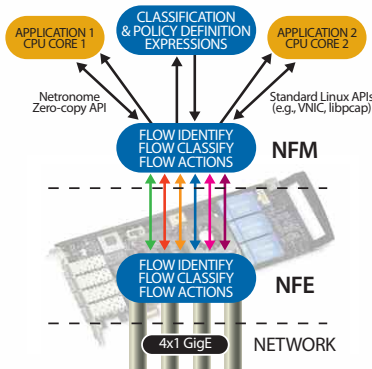
Intelligent
to the Core™

For more information about other Netronome products, please visit netronome.com.

Flow Processing

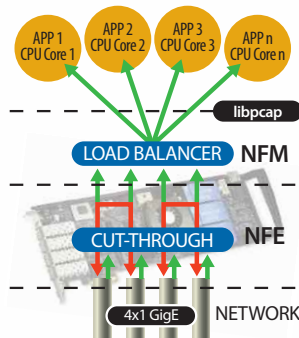
NFM also has the ability to apply actions to flows (classified by the 5-tuple within an application session), offering powerful, stateful flow analysis to applications. NFM allows active (inline/filtering) or passive (offline/capture) enterprise and networking applications to perform one or more unique actions on flows once they have been identified, including:

- “Cut-through”: All classified flows are switched through the appliance in hardware by the NFE
- “Load balancing”: Flows can be load-balanced across x86 CPU cores
- “Redirect”: All classified flows are diverted to the CPU for processing by the host application
- “Tap”: Flows are cut-through the appliance and copied to the host CPU(s) for further processing
- Tunnel Mode, where IP tunnels (e.g., GRE) can be terminated and re-originated, enabling the creation of virtual overlay networks
- Statistics and Monitoring mode, where NFM is used to gather detailed packet and flow level statistics and perform general application and flow monitoring



PCAP Load Balancing

As a complement to NFM’s broad set of DPI, cut-through and flow analysis capabilities, users can improve their application performance by load-balancing flows across x86 CPU cores support with flow-based adaptive load balancing to exploit multicore CPU parallelism. NFM uses a zero-copy interface to deliver packet or flow data from the NFE directly to Linux user mode applications, bypassing the Linux kernel and networking stack. To improve application performance in multi-core environments, Netronome has modified the libpcap packet-capture library to provide an interface to pcap-based applications to take advantage of the underlying acceleration hardware. Flows are balanced across CPU cores by computing a 3-tuple or 5-tuple hash key for common packet header fields.



Additional Features and Benefits

NFM 2.2 Hardware Support

HOST PLATFORMS

- NFM is compatible with a wide range of IA/x86 server motherboards and systems, including those from Intel®, AMD, Dell™ and HP. Please contact Netronome for a current list of supported host platforms

SUPPORTED HOST OPERATING SYSTEMS

- The NFM is compatible with all leading Linux environments, including Fedora and CentOS. Please contact Netronome for a current list of supported operating systems and versions.

SUPPORTED ACCELERATION CARDS

- Netronome Flow Engine NFE-i8000
- 12x1 GE Load Balancing Interface Module
- 4x10 GE Load Balancing Interface Module

NFM 2.2 Software Support

- Classifier API
- Graph configuration APIs
- Table-driven rules API (TCAM rules and SRAM action policies)
- Flow Modification API
- Pattern Matching and Utility APIs
- Statistics API
- Custom classification via arbitrary expressions for protocol-specific fields (e.g., HTTP URLs)
- Passive, Tap, or in-line packet capture modes with per port interface sets
- Multiple PCAP application packet delivery
- Load balancing to PCAP application instances – IPv4, IPv6, MPLS, GRE, non-IP packets (ARP)
- Parallel application voting
- Application-based packet modification
- Application software fail-to-wire
- Configurable errored packet delivery
- System health monitoring API
- System log API
- System troubleshooting API
- Software configurable fail-to-wire
- Port link control API
- Jumbo frame support



Intelligent to the Core.™

Netronome has operations in:

USA (Pittsburgh [HQ], Santa Clara & Boston), UK (Cambridge), Malaysia (Penang), South Africa (Centurion) and China (Shenzhen, Hong Kong)

info@netronome.com 877.638.7629 netronome.com