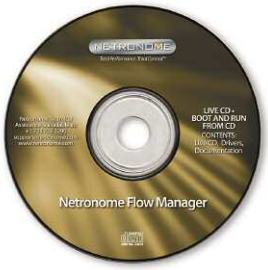
Total Performance.
Total Control.™

NETRONOME™

NETRONOME™ FLOW MANAGER (NFM)

As networking requirements continue to evolve, application performance and appliance scalability have become critical to helping IT organizations increase network bandwidth, deploy new applications, manage security threats and reduce operational costs. The Netronome Flow Manager (NFM), coupled with the Netronome Flow Engine (NFE), enables application acceleration, deep packet inspection and flow analysis in a highly scalable manner—addressing the needs of both developers and users of network appliances for significantly increased application performance and greater control over network traffic.



The NFM allows appliance manufacturers to quickly improve the performance of existing products, accelerate the development of their next-generation applications and reduce overall development costs. The NFM's capabilities are also ideal for end-users looking to accelerate the performance of their open source and custom-developed packet capture and packet filtering applications.

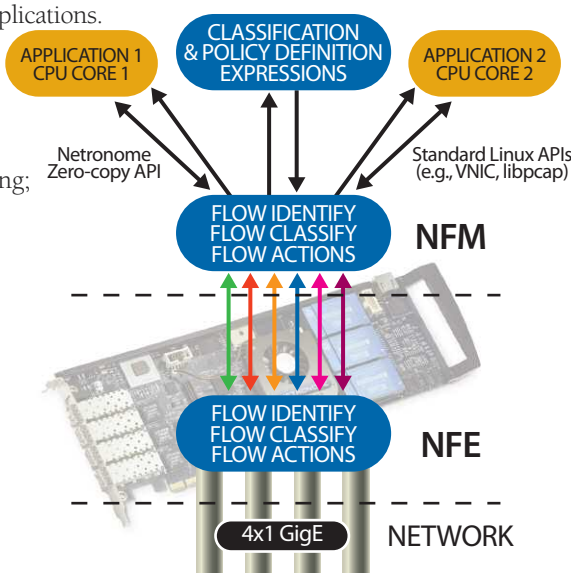
SIMPLIFIED ACCELERATION FOR NETWORK AND SECURITY APPLICATIONS

In addition to standard Linux® APIs, the NFM provides an open application programming interface (API) for network and security appliances and applications. The NFM significantly reduces appliance CPU utilization and packet delay/jitter by offloading complex flow classification and processing to the NFE. This provides appliance manufacturers and end-users with the ability to quickly improve the performance of existing network security applications and products, accelerate the development of their next-generation applications and reduce overall development costs. By abstracting complex NFE microengine programming with standard API calls, the NFM programming interface allows users to focus development on their software applications, while simultaneously benefiting from hardware acceleration that significantly increases performance. With the use of the NFM, network appliances can increase their application performance and I/O throughput without requiring modification to the existing applications or complicated programming of underlying acceleration hardware.

The NFM provides line-rate performance for a broad set of flow analysis and deep packet inspection capabilities, enabling unmatched visibility and control of application flows at Layers 2-7 for 1,000,000 simultaneous flows. In addition, NFM support for Netronome's Open Appliance Architecture™ allows network and security application vendors to quickly take advantage of these capabilities for their current Linux-based Intel® Architecture (IA)/x86 applications.

This unique combination of accelerated network performance, granular flow visibility and reduced time-to-market makes the NFM an ideal solution for network appliances used for:

- Security policy enforcement/compliance monitoring;
- Intrusion detection and prevention;
- Unified threat management;
- Deep packet inspection;
- URL filtering and reverse proxying;
- LAN/WAN bandwidth optimization;
- Application load balancing;
- Test, measurement and service assurance; and
- Lawful intercept (CALEA).



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

Granular Flow Analysis with Deep Packet Inspection

The NFM provides a full suite of L2-7 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 applications, such as BitTorrent, Gnutella, FastTrack, Jabber and WinMX.

Flow Processing

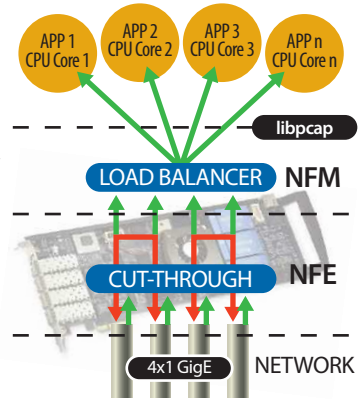
The NFM allows enterprise and networking applications to perform one or more unique actions on flows, once they have been identified, including:

- Flow Forwarding mode, where the appliance is deployed in-line, as a "bump-in-the-wire;"
  - "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.

Acceleration for Network Security Applications

In addition to the broad set of deep packet inspection capabilities offered by the NFM, users can improve their application performance by using a "zero-copy" mechanism to deliver packet or flow data directly to Linux user mode applications (bypassing the Linux kernel and networking stack) and load-balancing flows across IA/x86 CPU cores. Netronome has modified the libpcap packet-capture library to utilize the NFM capabilities, allowing pcap-based applications to take advantage of the underlying software and hardware. This approach frees the CPU(s) from the cycle-intensive task of getting packets from the Ethernet port to the application, extending NFM's capabilities to existing libpcap-based applications such as:

- tcpdump, a tool for capturing packets for further analysis;
- Wireshark (formerly Ethereal), a graphical packet-capture and protocol-analysis tool;
- SNORT®, a network intrusion detection system;
- Nmap, a port-scanning and fingerprinting network utility;
- Bro IDS, a network-monitoring platform; and
- Clam AntiVirus, an anti-virus toolkit designed especially for e-mail scanning on mail gateways.



Additional Features and Benefits

- A detailed flow processing API provides the ability to configure processing policies for each flow.
- A table-driven classifier (list of rules) simplifies the porting of applications that already use a list-of-rules mechanism, such as Linux iptables.
- Custom classification criteria can be implemented via arbitrary expressions that examine protocol-specific fields (e.g., extract HTTP URLs and pattern-match them), providing a level of expressiveness that is not possible with packet field ("n-tuple") rules.

SUPPORTED HOST PLATFORMS

The NFM is compatible with a wide range of IA/x86 server motherboards and systems, including those from leading manufacturers, such as 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, CentOS and Gentoo in both 32- and 64-bit variants. Please contact Netronome for a current list of supported operating systems and versions.

SUPPORTED ACCELERATION CARDS

Netronome Flow Engine NFE-i4000, NFE-i4010, NFE-i8000

SUPPORTED ACCELERATION APPLIANCES

Netronome Open Appliance OA-8041, OA-8082, OA-812x, OA-840x

NETRONOME™

Total Performance. Total Control.™

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
+1 877 NETRO A-Z
netronome.com