aria CYBERSECURITY SOLUTIONS

DATASHEET

Myricom® SNF® 10/25/100 GbE Packet Capture Software

High-rate packet processing, minimal CPU overhead, and open-source application support

The Myricom SNF high-rate packet capture software allows third-party DPDK-compatible network adapters to capture packets using a simple API. It is a tightly integrated combination of DPDK and user-level software libraries that enable sustained capture of Gigabit+ Ethernet traffic. SNF has the flexibility to configure advanced functions, leaving most server cycles available for your application requirements. Verified with NVIDIA® ConnectX® family and Intel® Ethernet network adapters to enable advanced networking applications.

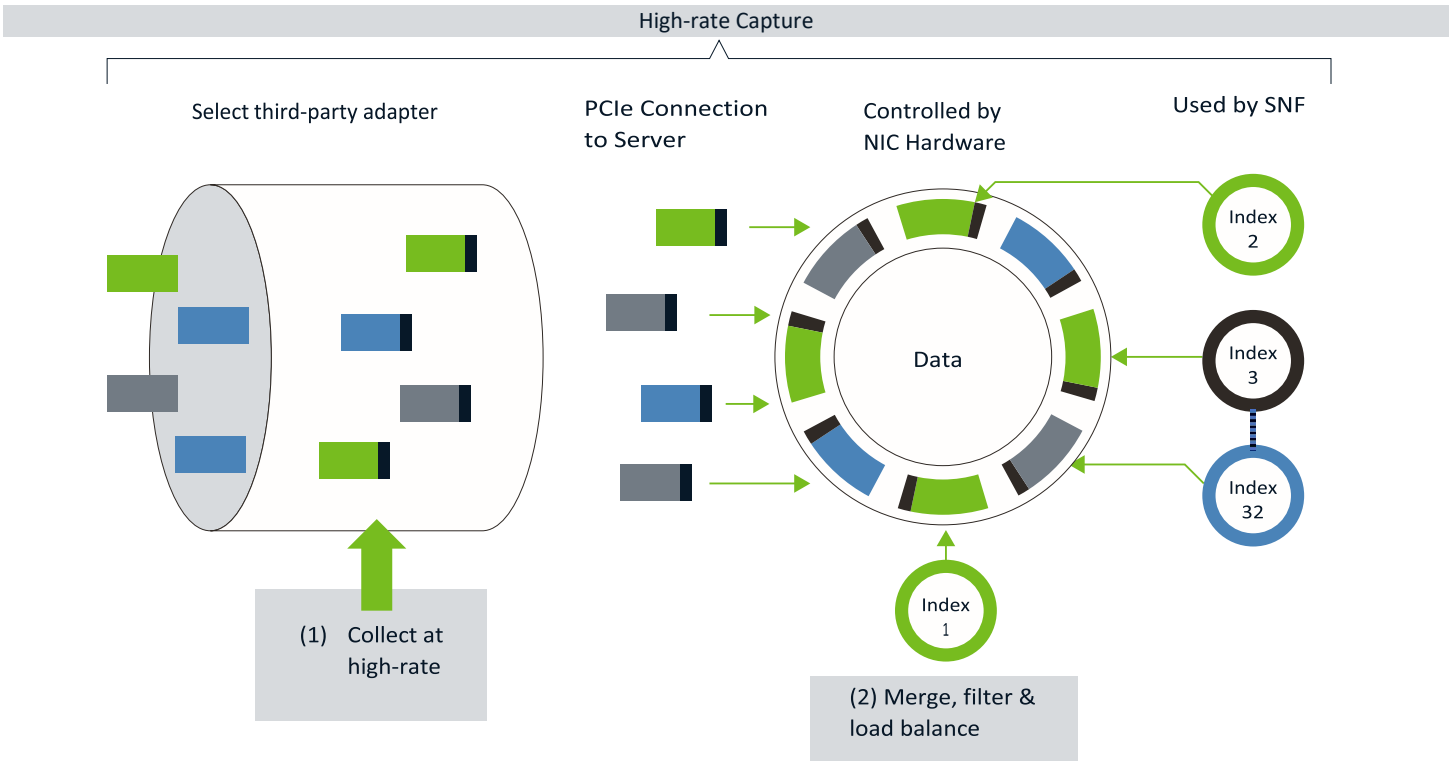
Key Features

- Complete visibility into what's happening on your network, critical for advanced threat detection and network security.
- High-rate packet capture across the full range of Ethernet packet sizes.
- Reduced CPU usage – SNF seamlessly sends all packets to the application, completely bypassing the OS kernel and freeing up CPU cycles.
- Low overhead – SNF allows you to capture multiple Gigabit+ Ethernet ports into a single server at maximum packet rate and still have enough CPU cycles available to run significant applications against these streams.
- Support for packet injection including reinjecting traffic that has been received on an interface.
- Node-locked licensing supports 10, 25 and 100 Gbps interfaces.
- Support for third-party, DPDK-compatible, 1, 2 and 4 port network adapters.
- Support for libpcap and a full set of open-source packet capture application tools.
- Adapter may be used as a general purpose NIC when supported by the third-party network adapter. No need for additional NICs for server application communication, which lowers costs.
- Support for Linux operating systems including Red Hat® and Ubuntu® based distributions.

High-rate Packet Capture

ARIA's Myricom SNF packet capture software allows popular third-party network adapters to deliver high-rate packet capture in support of critical network monitoring and security applications.

The SNF API includes a wrapper around the DPDK stack that simplifies the application code necessary to capture packets in user space. SNF packet capture capabilities can be leveraged through the SNF API, as a set of C programming language functions. SNF components are only active when the device is opened for capture through the SNF API.



Combining Cost-effectiveness, High Functionality, and Strictly Limited Server Impact

SNF handles high packet rates by bypassing the kernel altogether, thus offering unrestricted network traffic access to user space applications. SNF enabled applications gain full user space access to all incoming packets without any OS intervention—an important consideration when comparing SNF to other packet capture solutions.

SNF provides essential packet capture functions, including merging and load balancing. These functions can all be implemented with flexible application control using the SNF API or one of the industry standard libpcap libraries.

Flexible Multi-core Application Support

Using its flexible partitioning capability, SNF can engage all CPU cores in analyzing packets. Incoming TCP and UDP packet flows can be directed to multiple applications simultaneously, with each application controlling one or more

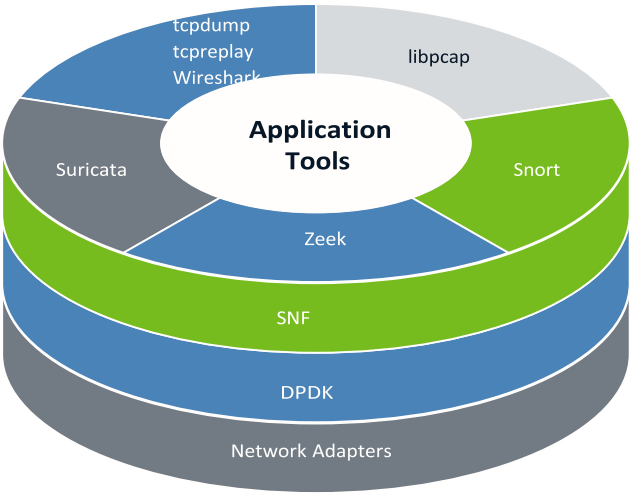
cores. SNF allows all applications to process the same packets simultaneously and frees up the packets only when every application has stopped using them.

Application developers can partition the packet flow across as many as 32 interfaces with the SNF API. With this capability, data flows can be balanced across multiple cores so each one analyzes an equal portion of incoming traffic. Developers can leverage user-defined rules from an application compiled to use the standard libpcap library. For applications that require deep packet inspection (DPI), this approach can reduce the processing time constraints under high packet rate loads.

Comprehensive support for common industry software

SNF can support open-source packet capture application tools. Some examples of tested applications include:

1. The standard Linux utilities tcpdump and tcpreplay
2. Wireshark network protocol analyzer
3. Zeek network intrusion detection system
4. Snort intrusion prevention systems
5. Suricata network intrusion detection and security monitoring



Deployment options that work best for you

SNF has been verified with NVIDIA and Intel high speed network adapters. It supports DPDK-compatible NICs allowing you to choose the best single, dual or quad port adapter and interface speed for your infrastructure.

SNF Software has been validated on the following third-party network adapters:	
10G	Intel Ethernet CNA X710-DA2
25G	nVidia/Mellanox ConnectX-4 MCX4121A-ACAT
100G	nVidia/Mellanox ConnectX-5 MCX556A-EDAT

SPECIFICATIONS		
Warranty	90 days for software defects. 90 days of "getting started" email support. 90 days of software upgrades.	
ORDER DETAILS	10G: 10G-SNFX-LIC 25G: 25G-SNFX-LIC 100G: 100G-SNFX-LIC	Node-locked license required to activate each interface.
OS Update Support	Optional support for future Linux OS versions. Contact your ARIA representative for additional information.	

Contact Us to Schedule a Technical Demonstration or Arrange an Evaluation ✉ **ARIAsales@ariacybersecurity.com**

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110
Follow Us: Linkedin • Facebook • Twitter

aria CYBERSECURITY SOLUTIONS

Myricom NETWORK ADAPTERS