

Myricom Sniffer10G - Integrated **FPGA** Firmware and **Software**

Delivering complete packet capture functionality in a cost-effective package

CSPI's Myricom® Sniffer10G technology powers the ARC Series of network adapters for packet capture, enabling advanced networking devices and applications without unnecessary costs. It is a tightly-integrated combination of FPGA firmware and software libraries.

Sniffer10G was designed to implement pure packet capture, with the flexibility to configure advanced functions so that they match application needs and perform efficiently, leaving the vast majority of server cycles available for your application.



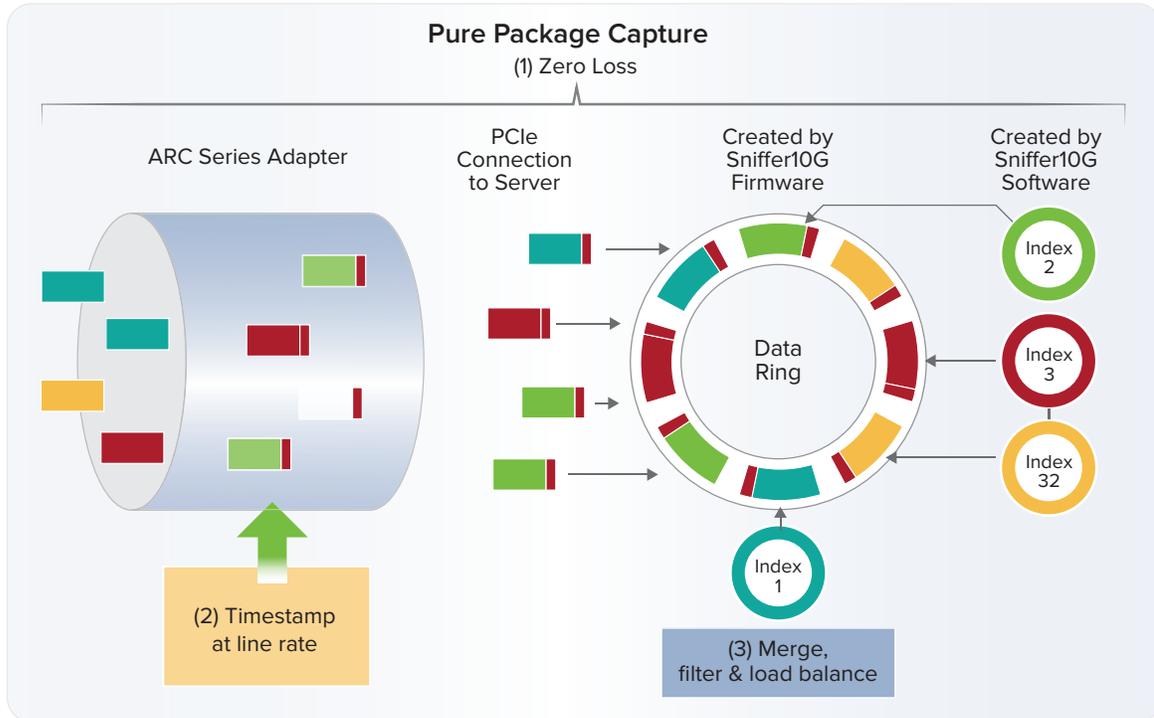
Pure packet capture

Today's network adapters must deliver on three areas of requirements for pure packet capture: (1) zero loss, (2) highly accurate timestamping and (3) essential packet capture functions.

A government study from Sandia National Lab* documents Sniffer10G's zero loss performance across a range of Ethernet packet sizes. This uncompromising quality results from an architecture that bypasses the kernel and sends packets directly into user space, leveraging a 'ring' that can expand to any size. As an application developer, you define ring sizes to rate match with your application.

Along with zero loss, Sniffer10G meets current network requirements by supporting packet capture and timestamping at line rate, up to the maximum possible rate of 14.8 million packets per second on each 10GbE line. The timestamping is also extremely accurate; ARC Series adapters contain high-quality clock crystals and users requiring extraordinary accuracy can connect to an atomic clock.

Sniffer10G also provides essential packet capture functions, including time-based merge, filtering and load balancing. These functions can all be implemented with flexible application control using the Sniffer10G API or one of the industry standard libraries: libpcap, WinPcap or PF_RING.



Flexible Multi-core Application Support

Using its flexible partitioning capability, Sniffer10G can involve 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. The adapter allows all applications to process the same packets and frees up the packets only when every application is done with them. Unique in the market, any application can be supported with its own specific data flow partitioning scheme.

Application developers can partition the packet flow across up to 32 rings using pre-built rulesets or implement user-defined rules with the Sniffer10G API. The API allows developers to meet application needs with partitioning based on virtually any criteria. With this capability, flows can be balanced across multiple cores such that each analyzes an equal portion of the incoming traffic. For applications that require deep packet inspection, this approach can relax the processing time constraints under high packet rate loads. Developers also have access to the complete Berkeley Packet Filter (BPF) language for filtering, unlike other adapters on the market which limit filters to a specified set of schemes.

Incoming traffic can be partitioned to multiple cores in a number of different ways including:

- Standard Flow Hashing: User selectable flow hashing based on Ethernet VLAN tags, IP, UDP headers, or TCP headers.
- GTP protocol hashing for mobile applications.
- Custom Hashing: A unique capability within Sniffer10G, this software defined hashing gives complete flexibility of selective packet forwarding to the application developer.

Sniffer10G solutions also offer advanced capabilities to address issues such as burst buffering and tunneling. This operational flexibility allows developers to implement application-specific optimizations and has already made ARC Series adapters with Sniffer10G the preferred solution in some market segments.

Cost-effective, high functionality and strictly limited server impact

The ARC Series network adapters are built to deliver extensive application flexibility while strictly limiting server overhead. Applications benefit from full user space access to all incoming packets without requiring any intervention from the OS, while routines called by the Sniffer10G API are optimized for performance. A cost-effective design approach balances feature implementation across hardware and software, with software using either industry standard libraries (libpcap, WinPcap or PF_RING) or the Sniffer10G API. The ARC Series adapters deliver a compelling combination – high functionality, acceptable server overhead, and price leadership.

Big Benefits for PCAP Users, Easily Implemented

By simply changing the linking library, users of libpcap and WinPcap can leverage Sniffer10G, gaining big benefits for packet capture applications. To simplify the implementations, Sniffer10G-capable libpcap and WinPcap libraries are included with the Sniffer10G software distribution.

Application advantages include:

- **Reduced CPU usage** – Sniffer10G seamlessly sends all packets directly to your application, completely bypassing the OS kernel and freeing up CPU cycles.
- **Lossless packet capture** – With Sniffer10G's user-definable ring sizes, applications can target a memory queue of any size. This flexibility eliminates packet drops due to rate matching challenges between hardware and software.
- **Applications in Parallel** – You can run multiple copies of libpcap against a single packet capture stream. This translates into multiple applications running simultaneously against the same packets, with zero copying in the background.
- **Exact time stamps** – ARC Series network adapters with Sniffer10G can provide timestamps with up to ± 0.5 nanosecond accuracy, using high-quality time signals attached via standard coax inputs.
- **Low Overhead** – Sniffer10G efficiency allows you to capture four 10 Gbit Ethernet ports into a single server with zero drops, at maximum packet rate, and still have enough CPU cycles available to run significant applications against these streams.
- **BPF** – Sniffer10G solutions fully support Berkley Packet Filters, every language feature, every corner case.



The Sniffer10G-capable libpcap and WinPcap libraries are Open Source enhancements developed by CSPi Myricom and are part of the standard source trees, as are our Linux drivers. CSPi Myricom provides both source and compiled versions of these software modules, which interface seamlessly with Sniffer10G.

Application	Most efficient tool
Passive packet capture	libpcap, WinPcap or PF_RING
Bump-in-wire security appliance	Sniffer10G API
Test equipment	Sniffer10G API

Comprehensive support for common industry software

Sniffer10G is also enabled with support for open source packet capture application tools. Some examples of tested applications include:

1. The standard Linux utility tcpdump
2. Wireshark network protocol analyzer
3. Bro network intrusion detection system
4. Snort intrusion prevention systems
5. Suricata network intrusion detection and security monitoring
6. PF_RING™ packet capture network socket, ported to run above the Sniffer10G API

User documentation includes configuration details for running these tools with the Sniffer10G software.

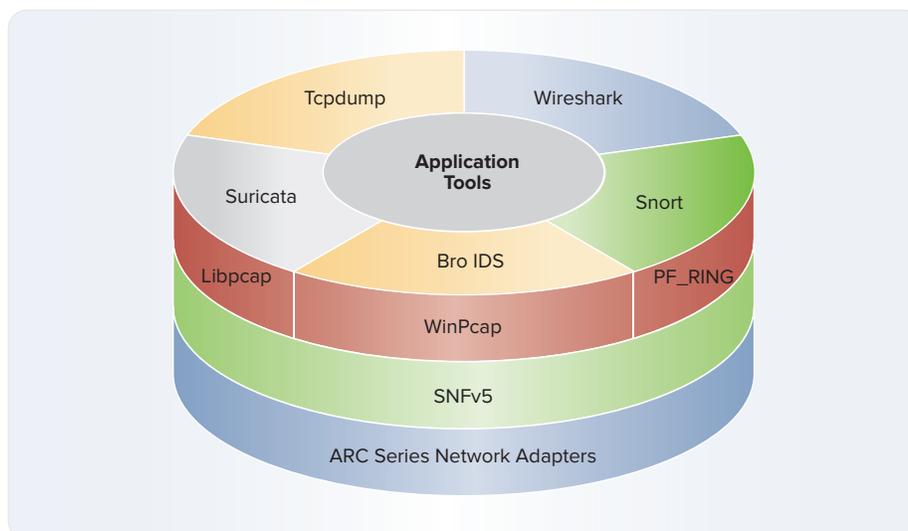


Figure 2 – Supporting Industry Standard Packet Capture Software



Enhanced Timing Features

Sniffer10G's integration with the ARC Series adapter hardware enables further flexibility with a set of advanced timing features, including:

- Timing synchronization:** PPS and 10 MHz connections are available (not on C-Class) to enhance timestamp accuracy by linking to external oscillators or GPS devices. One version of the ARC adapters offers an enhanced capability supporting ± 500 picosecond accuracy.
- PPS and 10 MHz daisy chaining:** Used for external time synchronization as well as synchronization across multiple modules for some adapters. Daisy chaining offers a straightforward way to enhance timing accuracy for applications with complex configurations.
- Support for Arista Networks DANZ timestamping:** Arista switches can optionally add timestamps to packet traffic flowing through the switch, using proprietary extensions to the IP standard that Sniffer10G software can decode. This allows applications to use the time packets entered a local network rather than the time they enter the network adapter.

Summary

Sniffer10G technology powers the Myricom ARC Series network adapters, delivering pure packet capture capability with zero loss, highly accurate timestamping at full line rate speeds and critical application support functions, including time-based merge, filtering and load balancing. Application developers can use Sniffer10G's unique capabilities to partition a data flow across up to 32 rings based on virtually any criteria.

To streamline application development, PCAP users can leverage Sniffer10G by just changing library links to the Sniffer10G-capable versions of libpcap or WinPcap. Sniffer10G also supports a full set of open source packet capture application tools as well as offering enhanced timing features.

Sniffer10G's optimized integration of FPGA firmware and software libraries strictly limits server impact while delivering a market-leading combination of functionality and flexibility – all with an aggressive price point.

About CSPI

CSPI (NASDAQ: CSPI) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPI Corporate Headquarters

175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPI High Performance Products

800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPI Technology Solutions

800.940.1111
us-ts-sales@cspi.com



www.linkedin.com/company/cspi-inc



[@ThisIsCSPI](https://twitter.com/ThisIsCSPI)



us-hpp-sales@cspi.com



www.cspi.com

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.