aria CYBERSECURITY SOLUTIONS

DATASHEET

The Myricom ARC Series of Network Adapters with Sniffer10G

Zero-loss packet processing, minimal CPU overhead, and open source application support – all in a cost-effective package that works for you

Features and Benefits

Zero-loss packet capture across the full range of Ethernet packet sizes.

Complete visibility into what's happening on your network, critical for advanced threat detection and network security.

Nanosecond scale time stamping at full line rate.

Ability to load balance packet delivery for up to 32 endpoints (e.g., CPU cores) based on user-defined rules.

Support for libpcap, **WinPcap, and PF_RING libraries** and a full set of open source packet capture application tools.

PPS and 10 MHz daisy chaining for multi-module time synchronization.

Ability to also use the adapter as a 10G general purpose NIC on port zero. No need for additional to a additional NICs, for server application communication, which helps keep costs down.

Building effective network sensors for your network security infrastructure requires the right combination of leading-edge technology, software plug-ins, and customer support. More, any hardware you choose must come with a proven track record and at a price that makes sense.

Today, network adapters play a crucial role within network sensors. They must manage high volumes of unrelenting network traffic without dropping any data packets, and then move this data into network analysis applications or recording devices as quickly as possible, without stealing away CPU cycles needed for application code.

CSPi's Myricom® ARC Series with Sniffer10G delivers. This series of multi-port network adapters provides pure packet processing as well as zero-loss reliability, user-defined functionality, and the ability to improve network security – representing a significant value over competitive products.

Close the Security Gap

If you are using off-the-shelf network adapters or other traditional hardware, you are missing a significant opportunity to optimize your next-generation security solutions. Without a specialized adapter, you are dropping packets and wasting valuable CPU time. This can make you more vulnerable to zero-day attacks and other threats to your network and data center.

Our Myricom ARC Series adapters improve threat detection with industry-leading designs that maximize network visibility and advanced threat detection.

Pure Packet Capture

Myricom ARC Series adapters with Sniffer10G implement pure packet processing by meeting three areas of critical requirements:

- Zero loss: A study from Sandia National Lab highlights 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, taking advantage of a packet buffer (or "ring") that can expand to any size for rate matching with software.
- Merge and load balance: Sniffer10G provides essential packet-capture functions. For example, ARC adapters can load balance (evenly distribute) IP flows among the many cores found inside the sockets of a host motherboard. ARC adapters can also merge both sides of a network tap, in timestamp order, into a single stream.
- Highly accurate time stamping: Accurate timestamps are needed for packet recorders and network test equipment. Applications can use these timestamps for precise indexing for highly accurate and quick searches. ARC adapters can timestamp incoming packets with the highest accuracy available anywhere. ARC adapters can also pace outgoing packets to that same degree of accuracy. ARC timestamps meet the most stringent accuracy requirements of MiFID II reporting. Latency measurements made using a single ARC Series E adapter can, with appropriate time signals, be accurate to ± 5 ns.

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

The Myricom ARC Series adapters deliver a compelling combination – high functionality, acceptable server overhead, and price leadership. ARC Series network adapters are built to deliver extensive application flexibility while leaving the vast majority of server cycles available for your application. This means applications will benefit from full user space access to all incoming packets without requiring intervention from the OS, while packets called by the Sniffer10G API are optimized for performance.

Additionally, a cost-effective design approach balances feature implementation across software and hardware. For example, software has the option of using industry-standard libraries (libpcap, WinPcap, or PF_RING) or the Sniffer10G API.

Flexible Multi-core Application Support

Using its flexible partitioning capability, Sniffer10G 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. The network adapter allows all applications to process the same packets and frees up the packets only when every application has stopped using them. Plus, using technology exclusive to ARIA Cybersecurity Solutions, any application can be supported with its own specific data flow-partitioning scheme.

Application developers can partition the packet flow across as many as 32 rings using pre-built rule sets or implement specific user-defined rules with the Sniffer10G API. This API allows developers to address application needs with partitioning models based on virtually any criteria. 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 API.

For applications that require deep packet inspection (DPI), this approach can reduce the processing time constraints under high packet rate loads. Your development team can also access the complete Berkeley Packet Filter (BPF) language, unlike other adapters on the market that limit filters to a specified set of schemes.

Enhanced Timing Features

The ARC Series network adapters provide a flexible set of timing features to meet a full range of application needs, including:

- Timing synchronization: PPS and 10 MHz connections are available (on E-Class) to enhance timestamp accuracy by linking to external oscillators or GPS devices.
- PPS and 10 MHz daisy chaining (E-Class only): Used for external time synchronization as well as synchronization across multiple modules. Daisy chaining offers a straightforward way to enhance timing accuracy for applications with complex configurations.

Choose the Model That Matches Your Requirements

The Myricom ARC Series network adapters are PCIe cards with tightly integrated Sniffer10G firmware and software libraries. Our two ARC Series product classes (our C and E Classes) are designed to offer the choice of features, functions, and capabilities that’s right for your objectives.

C-Class Features and Capabilities

C-Class provides a number of significant benefits and capabilities:

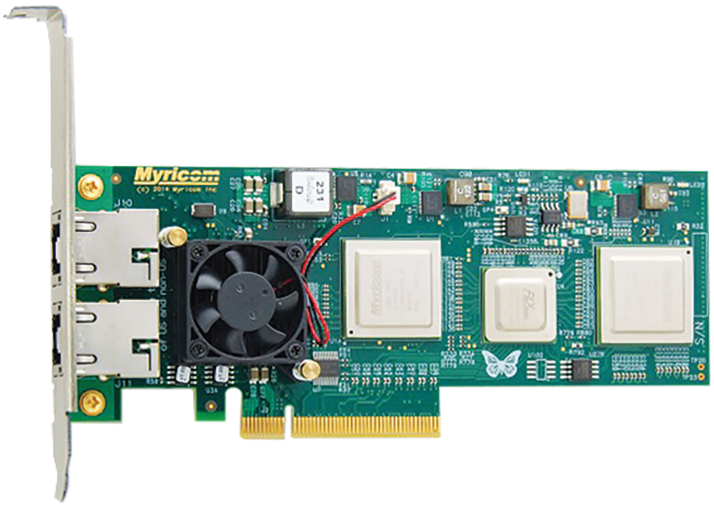
- Scales applications to work on multiple cores using built-in or user-provided algorithms
- Experiences no packet drops, even with extreme packet test sequences
- Requires less CPU overhead, delivering a CPU “frequency boost”
- Provides the ability to send the same packets into multiple applications without actually duplicating the packet data

- Creates time stamps on every packet with additional support for Arista switch time stamps
- Works under a libpcap interface, PF_RING, or using the Sniffer10G API
- Provides plug-ins for many popular open source applications, making the C-Class the most popular network adapter in those open source communities
- Works simultaneously as a standard NIC for those applications that do not require packet capture

E-Class Features and Capabilities

E-Class provides all the same functionality as C-Class as well as the following capabilities:

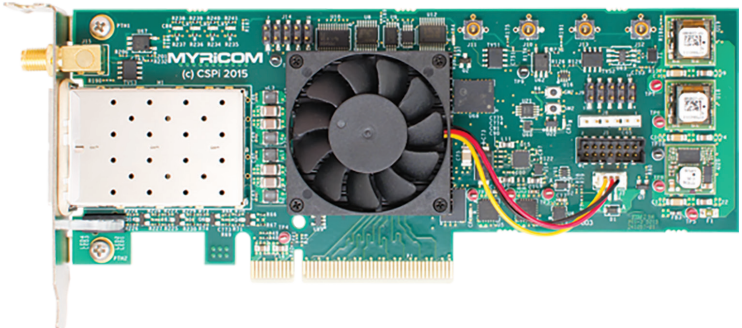
- Hardware offloading for scaling, including parsing capabilities for tunneling protocols like GTP/GRE
- Hardware offloading for port merging
- Extremely accurate timestamps and replay of packet recordings
- The ability to both capture and send malformed or bad packets, which is useful for network debugging and test equipment



C-Class

Features

- Industry's lowest cost pure packet capture device based upon the proven Myricom LANai ASIC
- Available in multiple form factors: low-profile PCIe, BladeCenter, and PC/104
- One or two 10G ports in either SFP+ or 10GBASE-T or XFP or CX4, the broadest range of 10G options on the market



E-Class

Features

- Very accurate time stamps as well as inputs for 1 PPS and 10 Mhz timing signals
- FPGA to enable a stream of future enhancements from CSPi
- Two or four 1 G or 10G ports using SFP+ cages (for bandwidths higher than 25Gbit, we recommend using a broker to load balance between ARC adapters)

ARC NETWORK ADAPTER FAMILY
KEY SPECIFICATIONS

Bus Interface	PCI Express Gen 3, eight (8) lanes wide.
Form Factor	All E Series ARC adapters are low-profile PCI Express x8 add-in cards that ship with a standard height faceplate installed and a low profile faceplate in the box. C-Class adapters are also available in BladeCenter and PC-104 form factors.
Electrical Power	25 watts or less for all models.
Environmental	Recommended that adapters be installed into servers that provide some airflow over the PCIe slots (very common). Use in an office or computer room environment. Rugged variants for telecom or defense applications are available.
Throughput	Sniffer10G provides 100% lossless packet capture and injection for all Ethernet packet sizes. Supports the maximum possible 10G packet rate of 14.8 million packets per second.
Timestamp Stability	Time stamp stability is determined by the on-board oscillator (a Vectron VT 804 TCXO) or by any optional, user-provided 10 MHz clock. The adapter has a 10 MHz input and repeater for connection with other modules.
IEEE 1588	Myricom time stamps are captured in a manner that allows IEEE 1588 software implementations to deliver highly accurate, synchronized time.
Software Support	The Sniffer10G packet capture capabilities can be leveraged through the popular libpcap (Linux) or WinPcap (Windows) library or directly through the Sniffer10G SNF API, which is available as a set of C programming language functions. Using a SNF-aware libpcap/WinPcap, users reference a Myricom ARC Series 10G network adapter through its Ethernet interface name, and can run existing libpcap/WinPcap-dependent applications, relying on libpcap/WinPcap's portable interface. For more advanced usage, the SNF API can be directly targeted by user applications. In both usage cases, network access via the SNF interface to the ARC Series 10G network adapter, rather than via the standard kernel access, provides higher performance.
Connections	**C-Class:** Dual SFP+ 10GbE ports; 10GBase-T, XFP and CX4 available on some versions. **E-Class:** Dual or Quad SFP+ 10GbE ports.
REGULATORY APPROVALS, COMPLIANCE	
Emissions	Emissions and safety authorities do not certify board-level products. They certify complete systems with all boards installed. To minimize risk for OEM customers, CSPi uses a third-party certification organization to test its Myricom adapters installed into a generic PC. Final test reports are available to customers. We meet US, Canadian, and European emissions, Class A.
Compliance	RoHS (Reduction of Hazardous Substances)
Country of Origin	USA
OTHER DETAILS	
Cables and transceivers	Contact your account/sales representative for more information on cables and transceivers that are compatible with each adapter.
Warranty and add-on support	One year for hardware defects, and 90 days for software defects. Ninety (90) days of "getting started" telephone and email support as well as any software upgrades shipped within that window. Refer to the support datasheet for options extending the 90-day window.

Software Configuration Flexibility

In addition to using the Sniffer10G API, the ARC Series' packet capture capabilities can be leveraged through the industry-standard libpcap/WinPcap libraries. To simplify these implementations, Sniffer10G-capable libpcap and WinPcap libraries are included with the Sniffer10G software distribution. PF_RING is supported by third-party ntop for Linux distributions.

Sniffer10G is also enabled with support for open source packet capture application tools, including:

- ZEEK IDS
- Suricata
- Wireshark & tcpdump
- Snort
- nProbe (plug-in sold by ntop)
- Moloch (plug-in included)

Please refer to user documentation for configuration details related to running these tools with the Sniffer10G software. Most software packages are validated using the Myricom build of libpcap/WinPap without need for a plug-in.

Summary

The Myricom ARC Series network adapters with Sniffer10G deliver pure packet capture capability with zero loss, highly accurate time stamping at full line rate speeds, and essential packet capture functions, including time-based merge and load balancing. Multi-core application support is enabled by a uniquely flexible partitioning capability. Impact on server performance is strictly limited. Enhanced timing features are supported as well as industry-standard libraries and open source application tools.

Contact Us Today: sales@ariacybersecurity.com or 800.325.3110

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 / Linkedin / Facebook / Twitter / Blog