Sniffer10G Packet Capture and Injection

Used for Lawful Intercept and inside Cybersecurity Appliances

Sniffer10G software, running on CSPi's Myricom® 10-Gigabit Ethernet adapters, provides enterprise and government customers and partners the ability to capture, inject, and analyze network traffic at line rate (up to 20Gbps for a two-port adapter) for all Ethernet packet sizes, with low host-CPU overhead. Sniffer10G serves the following market segments: network surveillance, monitoring and analysis; test, measurement and packet generation; deep packet inspection (DPI); and as a critical technology component within distributed denial-of-service (DDoS) defense appliances.

Flexible Multi-core Operation

Sniffer10G can involve all CPU cores in analyzing packets in two ways: with partitioning and/or with duplication. With partitioning, incoming TCP and UDP flows are balanced across up to 32 receive rings such that all cores (up to 32) can each analyze 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. With duplication, all incoming packets are made available concurrently to multiple rings such that each core can use different criteria when analyzing the same data.

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

- 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 – software defined hashing gives complete flexibility of selective packet forwarding to the application developer.

Sniffer10G supports multiple simultaneous applications. Duplicate traffic can be provided to multiple applications running on user configurable host cores.
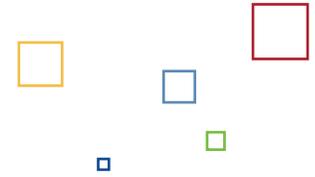
KEY FEATURES

- Sniffer10G enabled Myricom adapters provide a zero loss packet sniffing and injection security solution

- Sniffer10G based solutions reduce CPU overhead, leaving more server cycles for the application

- Myricom adapters DMA packets directly into user space, bypassing the kernel to lower overhead

- Supports Arista Networks DANZ time stamping

- Multiple cores or applications can process the same packets without data duplication

- Supports Libpcap/WinPcap

- Flexible Multi-Core Operation

MYRICOM

Products by CSPi

Product Specifications

KEY SPECIFICATIONS	
Bus Interface	PCI Express Gen 2, 8 lanes wide (dual port adapters) PCI Express. Gen 1, 8 lanes wide (single port adapters)
Form Factor	Low-profile PCI Express x8 add-in card. Ships with a standard height faceplate installed; low profile faceplate in the box.
Electrical Power	14.5W - 17.7W, Dual Port Adapters 14.8W - 18.0W, Timecode Enabled Adapters 3.9W - 5.6 W, Single Port Adapters
Environmental	It is recommended that adapters be installed into servers that provide some air flow over the PCIe slots (very common). Use in an office or computer room environment.
Throughput	Sniffer10G provides 100% lossless packet capture and injection for all Ethernet packet sizes. Supports the maximum possible 10G packet rate of 14.88 million packets per second.
Latency	Sniffer10G adaptive packet coalescing enables very low latency during normal traffic conditions and limits actual latency during extreme traffic conditions. The worst case latency for standard (1500 byte) frames is 4 microseconds.
Timestamping	Sniffer10G supports Arista Networks DANZ time stamping which enables the Arista 7150S switch hardware to time stamp every packet. This maximizes analysis accuracy and resolution by placing the time stamp closest to the actual traffic path, removing queuing and jitter typical in multiple input analysis networks. Sniffer10G also operates on Myricom's Timecode Enabled Network adapters which are fully compatible with IRIG-B00X time formats and provide precision time stamping capability independent of the Ethernet network.
Operating System	Support for all major Linux distributions as well as Windows 2008R2 and newer.
GPU / Third-Party Accelerator Support	Sniffer10G enables registration of the Sniffer10G zero-copy data ring to better interoperate with third-party accelerators such as NVIDIA's GPU platforms. Applications using NVIDIA's CUDA API can transfer Sniffer10G data to the GPU without an intermediate host copy, reducing host CPU overhead.
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 Myri-10G network adapter through its Ethernet interface name and then 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 Myri-10G network adapter, rather than via the standard kernel access, provides higher performance.
REGULATORY APPROVALS, COMPLIANCE	
EMI and EMC, Class A	USA, Canada, Europe, Australia/New Zealand, and Japan. Test reports are available upon request.
Compliance	TAA, RoHS (Reduction of Hazardous Substances)
Country of Origin	USA
PART NUMBERS	
10G-PCIE2-8CS-2S+SNF3	Network adapter with Dual SFP+ 10GbE ports and Myricom Sniffer10G software.
10G-PCIE2-8CS-2S-SYNC+SNF3	Timecode enabled network adapter with Dual SFP+ 10GbE ports and Myricom Sniffer10G software.
10G-PCIE-8B-S+SNF3	Network adapter with Single SFP+ 10GbE port and Myricom Sniffer10G software.
Warranty and add-on support	Three years for hardware defects and 90 days for software defects. 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.

CSPi
High Performance Products