

cPacket Networks
2061 Landings Drive
Mountain View, CA 94043
www.cpacket.com

For more press information contact:

Abigail Johnson/Paul Michelson
Roeder-Johnson Corporation
(650) 802-1850
<http://email.roeder-johnson.com>

For more customer information contact:

cPacket Networks
Mountain View, CA
+1 (650) 969-9500 FAX: +1 (650) 969-4900
info@cpacket.com

**BEYOND DEEP PACKET INSPECTION: NEW CHIP FIRST TO PERFORM "COMPLETE" PACKET INSPECTION,
AT WIRE SPEEDS TO 20 GBPS AND BEYOND**

**Breakthrough Processing Architecture Outperforms Existing Best-of-Breed Traffic
Analysis by 10x; Low Cost, Low Power Enables Embedding in Any Switch - from
Enterprise and Service Providers to Small Office**

MOUNTAIN VIEW, CA - May 14, 2007 - cPacket announced today a new chip that can perform "complete packet inspection" - a combination of "deep packet inspection" plus header classification - and can do so at an unprecedented 20 gigabits per second at 6 Watts. The chip makes possible "intelligent" network switches, routers, or network devices that are able to actively analyze and respond to network traffic based upon a 100% analysis of the packet payloads as well as the headers. It offers as much as 10 times the processing performance, for one-tenth the cost, of today's extremely complex and expensive solutions.

The 100-to-1 breakthrough in system cost-performance is so significant that complete packet inspection - and the intelligent network devices that it enables - has the potential to become pervasive, not only at the network perimeter, but in LAN switches, line cards, blade servers, and even in SOHO equipment. Use of the chip both in existing designs and high-value-added new products is greatly simplified by its "bump in the wire" integration model. It is supported by a simple but powerful template-based application programming interface (API).

Deep packet inspection is the network equivalent of United Parcel Service opening and inspecting the contents of every package entering any of their facilities, and then differentially handling each package based on its contents. For example, perishable goods might be identified, hazardous materials redirected, and terrorist threats contained, with accompanying alarms.

Clearly such 'deep' package inspection would be a massive, complex, and expensive undertaking for UPS that could have unpredictable effects on throughput. "In the network context, it is no different," said Rony Kay, cPacket founder and CEO. "Today, only applications that have tremendous financial or strategic impact - to the end users or to the service providers - can justify the cost of the capability of inspecting, analyzing and reacting to every bit in every data packet."

What cPacket has done is invent a way to inspect and classify packets based on both the payload and the header, simultaneously, at "wire speed" of 20 gigabits per second and beyond. Packets that match profiles provisioned to the chip by the simple provisioning software can be counted, tagged, redirected, replicated or dropped.

The patent pending architecture of the chip is such that the processing throughput is completely deterministic - that is, independent of the data - making exact throughput guarantees possible, a feature that designers and product managers will appreciate. In addition, the unique algorithm allows the throughput to scale linearly with the chip area to 40 and 100 gigabits per second (Gbps).

-more-

The chip being announced today is designed for 20 Gbps aggregated bandwidth, or 10 Gbps full duplex, operation regardless of packet size. The chip forms the heart of cPacket's quietly-unveiled and field-tested full hardware and software reference design (see: "[See Packet. See Packet sit. cPacket Run!](#)", Robert Ballecer, INTEROP Blog).

Complete Packet Inspection

cPacket's Complete packet inspection chip combines programmable general purpose header classification and payload pattern searching - including native support of wildcards, don't-cares, ignore-case, non anchored searches, etc. - without using any external memories or other components.

With the explosion of bandwidth-hungry and performance-sensitive applications such as video, or IP telephony, and the simultaneous growth of network security threats such as worms or targeted attacks, network architects and administrators require much finer-grained control of their networks. Ultimately, they seek an infrastructure that will allow the network to monitor itself, and react to issues dynamically, like the human body's immune system reacts to changing environment or infections.

Today, solutions for such "behavioral traffic analysis" and deep packet inspection in so-called "intelligent" networking equipment rely upon multiple components and parallel architectures that consume large amounts of power, and those solutions can be 10x more costly than the underlying packet switching infrastructure. This goes counter to all other trends in the network: 1 gigabit per second ports are becoming commoditized, and a 24-port managed gigabit switch with two 10 gigabit uplinks will probably cost under \$2,000 within 12 months. Clearly, adding deep packet inspection and analysis for \$50,000 to \$150,000 - today's price for 20 Gbps capability - is grossly out of sync with such trends.

What is really needed is a pervasive solution that not only performs complete packet inspection at commodity prices in every range of equipment, but also allows active control of the traffic by that equipment. This is what cPacket has accomplished.

cPacket's unique algorithms and chip architecture support on-the-fly inspection of every bit in every packet at full line rate, including worst-case conditions like minimum size packets. The fully pipelined architecture comprises of two-dimensional array of proprietary VLIW processing elements that provide predictable throughput under any traffic conditions. It is different from existing solutions that address some average "normal" behavior, but do not cope well with traffic condition that happen in actual worst case scenarios.

For example, the cPacket chip makes it possible to analyze spikes and micro bursts that can cause intermittent network congestion and temporal TCP back-off that negatively impact end users. It can also be used for monitoring events like failed login attempts and for taking mitigating actions by dropping or rate-limiting specific traffic profiles. Simple template based provisioning allows users to specify complex traffic profiles without worrying about low level protocol details like chained VLANs, IP options, or non-anchored case insensitive pattern searches.

Complete Packet Inspection enables integration of traffic monitoring, network security, test, and lawful intercept into intelligent switches and network devices.

cPacket will provide the chip, software application programming interface (API), and reference designs with different physical interfaces as a complete package. Original equipment manufacturers

interested in sampling the chip, or discussing subsystems based on the chip, should contact cPacket directly.

About cPacket

cPacket Networks is an emerging leader in chips and technologies that offers breakthrough, "complete" packet inspection, at a fraction of the complexity, power, or cost of preexisting approaches. It provides manufacturers of routers, switches and other network appliances a low-impact means to easily drop game-changing, wire-speed active network traffic analysis and response directly into their existing or planned designs - whether targeted at the service providers, the enterprise, or the small office. The exploding use of networks for media-centric applications makes the availability of truly pervasive deep packet inspection timely and crucial.

cPacket was founded in 2003 and is located in Mountain View, CA. For more information, visit www.cpacket.com.

-30-

Editors, note: All trademarks and registered trademarks are those of their respective companies.

Additional background information is available at www.roeder-johnson.com.