cVu Traffic Monitoring Switches

Complete Packet Inspection and L2-L7 Filtering
Aggregation, Flow Balancing, Performance Monitoring

Multiple Form Factors 12/24/32 x 10G/1G ports (SFP+/SFP)

One-to-many, Many-to-one, Many-to-many

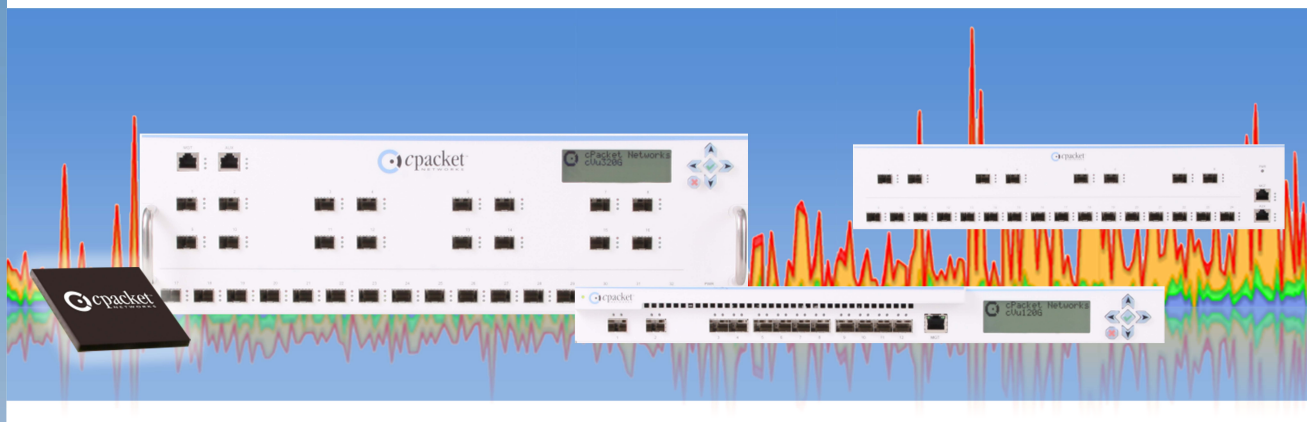
Complete Packet Inspection of Every Bit in Every Packet

Automatic Flow-based Load balancing

Real-time performance info and plots

On-the-fly reporting of microbursts and spikes

Open format for data export and Auto-Triggers



Successful data center and network operations rely on proactive monitoring and implementing corrective actions. cPacket's cVu Traffic Monitoring Switches serve as a central "tools hub" providing flexible traffic access to monitoring, trouble shooting, and security tools. They provide advanced built-in performance monitoring with real time reports, historical trends, and microburst detection. Based on Algorithmic Fabric Custom Silicon and a unique hardware-software architecture, the cVu family delivers best in class feature set and ease of use.

The impact of high speed traffic on monitoring and security tools is like drinking from a fire hose. The overwhelming volume of data drowns out telltale signs that would trigger a proactive response. Insufficient network visibility and situational awareness leads to intermittent network behavior, application performance issues, and service disruptions. The "hub" provides real-time reports of key performance indicators combined with flexible forwarding, balancing, and filtering based on complete packet inspection of header fields and payload content. User configuration is supported from both a browser-based Graphical User Interface and a programmatic command line.

The product family includes several form factors and port configurations from 12 to 32 ports for a range of deployment needs. Multiple devices in a virtual stack can be managed from a unified interface. Incoming traffic is inspected in real time by L2-L7 filters at line rate, combined with the traffic from any other input ports, and steered to any output port in a flexible any-to-any topology. Pre-filtered traffic feeds into downstream tools or, optionally, is tunneled to a remote location over a routed network to enable distributed visibility with a centralized set of tools. The cVu can partition traffic to a cluster of downstream elements based on static or dynamic flow balancing policies. It can also time stamp packets immediately at the input transceiver before queuing, buffering, or switching, which is the most accurate and scalable approach for latency measurements. Additional features include packet slicing, dynamic TCP payload masking, MPLS stripping, and packet de-duplication.

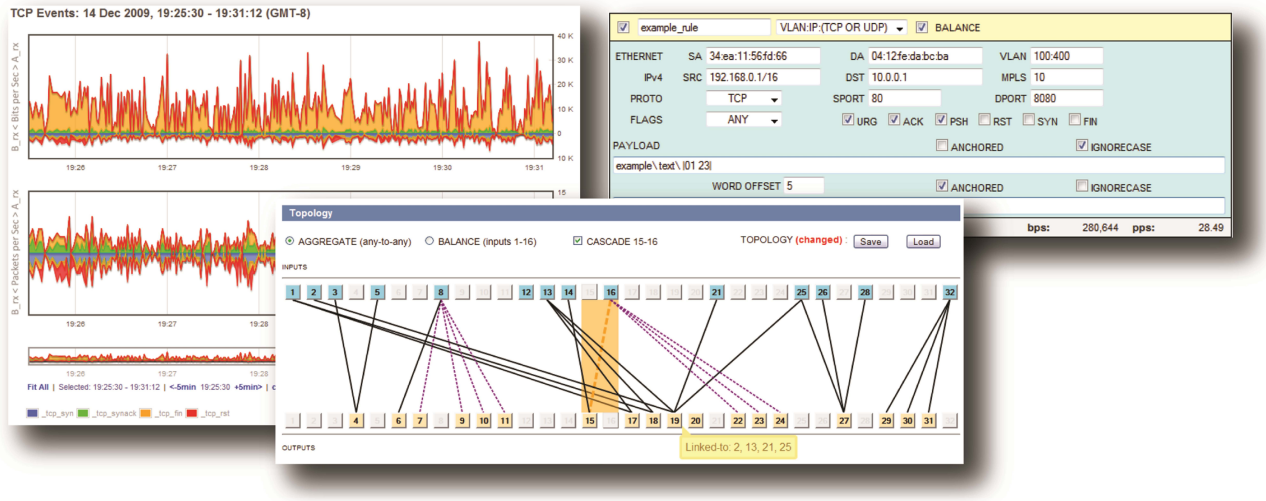
The graphical user interface allows network operators to specify filters based on complete packet inspection of every bit in every packet and every flow including pattern search anywhere in the payload. This complete inspection is performed at full 10 Gbps line rate per smart port, deterministically, under any traffic conditions. Payload patterns may include wildcards and don't cares.

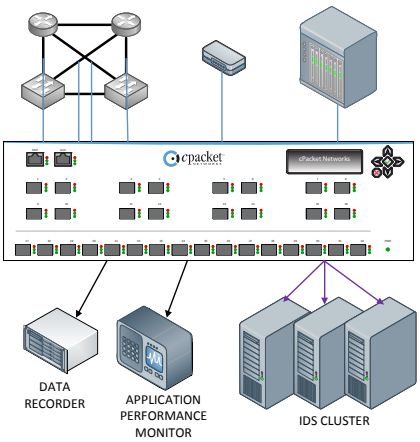
Built-in and user-configurable counters provide second-by-second performance information in a graphical dashboard and standard CSV files that can be imported by other monitoring frameworks. High resolution drill down into microbursts and spikes reveals micro-behaviors, which are overlooked by other tools and are frequently the cause of intermittent packet loss or other "unexplained behaviors". Automatic triggers can generate alerts for unusual traffic conditions or behavioral anomalies on your network.

Key Features

- Complete packet inspection of packet headers and payload anywhere in the packet at full 10 Gbps line rate per port
- Traffic aggregation in one-to-many, many-to-one, and many-to-many topology configurations
- Predefined and automatic load balancing policies including automatic flow balancing with hot stand-by and fail over
- Detailed network and application performance monitoring with second-by-second bit and packet counters
- Web access to snapshots of packets captured for specific user defined traffic profiles
- Forwarding of filtered packets to remote destinations enables distributed or centralized deployment models
- Built-in precision microburst analysis
- Automatic triggers and alerts of behavioral anomalies and threshold violations
- Accurate time stamping directly at the input PHY with sub-microsecond accuracy with digital PLL and diagnostics
- Clock synchronization to absolute time reference to enable time stamping for accurate one way latency measurement
- Historical access (visual and CSV) to second by second behavioral data for post analysis or drilldown
- Stacking of devices to aggregate, filter and monitor a large number of links over a common GUI

Topology Dashboard, Complete Packet Inspection (L2-L7) Filters, and Performance Visualization





CVU PRODUCT FAMILY			
Interfaces	12 x 10G (SFP+/SFP), 1 x management (RJ45)	24 x 10G (SFP+/SFP), 1 x management (RJ45)	32 x 10G (SFP+/SFP), 1 x management (RJ45)
Dimensions (H x W x D)	1.73” x 17.4” x 23.0” rack mounted chassis	3.5” x 17.4” x 23.6” rack mounted chassis	5.2“ x 17.5” x 23.6” rack mounted chassis
Weight	20 lbs	32 lbs	43 lbs
Power	300 W	400 W	500 W
	DC Power Option Available Redundant hot-swap supply		
Operating Requirements	0 to 40° C, 32 to 104° F		
Certifications	FCC Class A, EN 55022 Class A		