cpacket NETWORKS

Tech Brief

Two-Tier Network Monitoring Architecture

A Scalable Approach for 100Gbps Deep Packet Inspection and Comprehensive Network Visibility

Technology Benefits

- Lossless 100Gbps Monitoring Architecture

  Provides port density optimization and network packet inspection

- 100Gbps Packet Capture and Storage

  Line-rate packet storage and retrieval

- Performance Optimization

  Isolating the core network from the tools

Business Benefits

- Reduced downtime

  Operational teams gaining the advantage with greater visibility

- Optimizing Cost

  Separating packet acquisition and aggregation from packet delivery enabling processing where it's needed

- Operational Efficiency

  Pervasive visibility allows you to optimize applications, security posture, and network capacity

The Challenge

Data center consolidation and refresh are driving the need to migrate to 100Gbps speeds due to its economies of scale. It usually starts in the north-south direction by consolidating the data center interconnect (DCI) or WAN-edge from Nx10Gbps to fewer 100Gbps links. Eventually, the increased east-west traffic driven by intensive applications and growing data triggers the compute and storage bandwidth upgrades, pushing for 100Gbps within the data center spine-leaf LAN and SAN.

As the data plane gets upgraded to 100Gbps, it is simply not possible to upgrade or deploy existing TAPs (Test Access Point) to 100Gbps or TAP every link at those speeds. It would be an expensive and complex proposition. Even to TAP a percentage of links for network monitoring, a scalable and economical 100Gbps aggregation solution would be required. Moreover, many application-performance-monitoring (APM), security tools such as IDS/IPS, and SIEM systems are still not supporting 100Gbps and staying at 10/40Gbps speeds. Therefore, a multi-speed distribution layer interfacing to the tool-rail is required.

The most critical challenge is to ingest, process, and replicate the data at 100Gbps speed without dropping any packets. Every network packet passes by in 6.7 nanoseconds at 100Gbps – that is fast. A rock-solid packet brokering solution is required to process those streams of packets so that the tools can rely on a dependable data delivery to make the decisions they need to make. Otherwise, tools would make erroneous decisions and misleading alerts based on partial visibility.

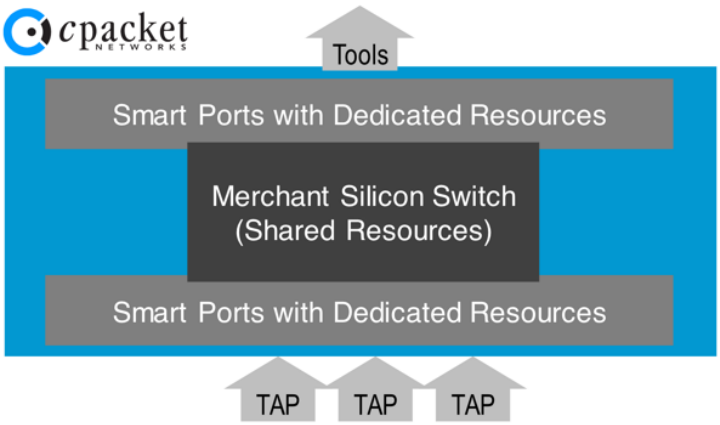
These challenges get stretched further in low-latency networks due to microbursts and sensitivity to network congestion. Some of the latency monitoring needs to happen closer to the source of the data versus after passing through one or two packet brokers.

The above rather distinct roles of aggregation, distribution, and packet-processing would not be possible to be squeezed into a single box and requires a more thoughtful architecture that would scale with the traffic.

The Technology

The technology required for distribution and aggregation is a way to separate those two functions, put the processing power precisely where it is needed, and reduce the over cost of the monitoring fabric. The aggregation and distribution layers require a lower price per port with higher port density and diversity. It needs to connect many 100Gbps ports facing the data plane and connect a mix of 10/25/40Gbps ports on the data plane and tool rail. It would handle the features such as terminating VXLAN or ERSPAN tunnels, load-balancing and replicating the packets to multiple destinations without overburdening the costs. This is why the cPacket cVu® 32100/32100E packet brokers that have lower costs are ideal for this usage.

The core monitoring layer needs to be more sophisticated; it is required to process and manipulate packets with features such as packet slicing, truncation, deduplication, as well as microburst and latency monitoring. cPacket cVu 16100NG next-gen packet broker+ is an ideal solution here. The cVu 16100NG is a 2-in-1 device: an advanced packet broker as well as a monitoring tool. The FPGA-based 'smart ports' on a cVu 16100NG process the traffic up to 100Gbps using purpose-built silicon dedicated for processing line-rate per port. cVu 16100NG has a dedicated FPGA space for each port which makes it highly versatile and powerful. Due to this distributed processing architecture, cVu 16100NG does not suffer through the processing bottlenecks or packet loss issues that many other packet brokers suffer through. Read about cPacket NG-series NPB Architecture.



cPacket Technology – full visibility

- cPacket: Meters, Processes, Filters
- Reports on every packet
- Processes the packets
- Filters unneeded packets out before the funnel

Both cVu 16100NG and cVu 32100E support the cPacket cBurst® feature, that characterize the link utilization for the connected tools for over or under-provisioning and capacity optimizing the WAN edge – maximizing the returns on investment. The cBurst feature can also be used for microburst characterization, which is critical for ultra-low-latency environments. The cBurst feature leverages hardware signaling to gain access and visibility to specific flows available for trending and provides visualization through dashboards. Unlike measurement methods that rely on proxies such as buffer utilization, the cBurst feature measures for each profile and the network behavior at millisecond resolution. Moreover, it does this in real-time for up to 1,000 flows per link regardless of the network traffic speed or the packet mix. Read more about cBurst.

Isolating the core network from the monitoring and security tools provides IT greater flexibility for availability, serviceability, scalability, performance, and visibility. Tools tend to grow over time as providers update and refresh to accommodate growth and greater network speeds. Using TAPs and Network Packet Brokers (NPB) allows us to make changes and scale both the core and tool architectures independently. Real-time packet processing gives the user control over packet sizing and distribution.

The Solution

cPacket provides scalable and cost-optimized packet brokering at 100Gbps for aggregation of TAP and SPAN (Switch Port Analyzer) ports and high-performance packet brokering for security delivery and network monitoring services. Separating the monitoring and security tools from the core data plane provides operational teams greater flexibility for packet flow analytics, network packet services, and troubleshooting production incidents with interactive data visualizations and fabric management all in a single-pane-of-glass.

Diagram 1 shows a well-designed Two-Tier monitoring and brokering architecture required for high-speed core networks, including the aggregation and distribution monitoring layers. cVu 32100 or cVu 32100E are used for the aggregation – for the generic vs. low-latency networks respectively. Both support 32 ports at up to 100Gbps and low-latency cut-through switching. The cVu 32100E supports some additional features such as cBurst with precision timing. Read more about cVu series in the datasheet. The cVu 16100NG includes 16 multi-speed ports and supports a lot more features. See cVu series datasheet or cPacket Product Quick Reference Guide for the comparison.

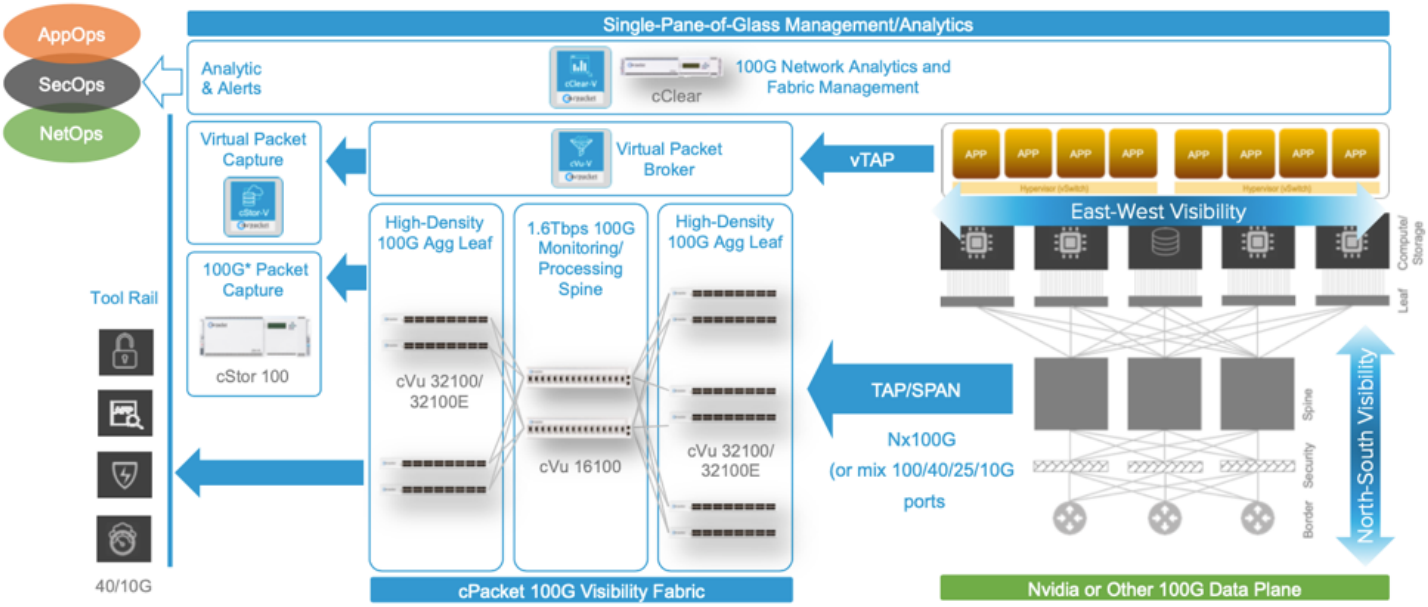


Diagram 1 – cPacket Two-Tier Monitoring & Brokering Architecture

The Two-Tier visibility fabric is designed to facilitate 100Gbps migration or future proofing in data centers, trading exchanges, and HPC clusters with backward compatibility. It scales with any data center network fabric from any vendor, including but not limited to Cisco, Juniper, Nvidia, Arista, Extreme, Dell, HPE, and others. To round out the solution, the cPacket cStor® series packet capture devices can be added to receive the packet data feed from the Two-Tier visibility fabric and archive those packets permanently for the historic analysis, troubleshooting, or stateful protocol analysis including TCP analysis, RTP analysis, and market-data-feed gap detection.

For overall provisioning, management, and observability of holistic cPacket devices in the architecture, cPacket cClear® provides customizable dashboards. Diagram 2 shows a typical port trend visualization using cClear dashboard examples, including "Maximum Burst" (green), "Average Burst" (yellow), and "Baseline Max Burst" (blue). Alerts can be enabled based on delta value triggers from baseline.

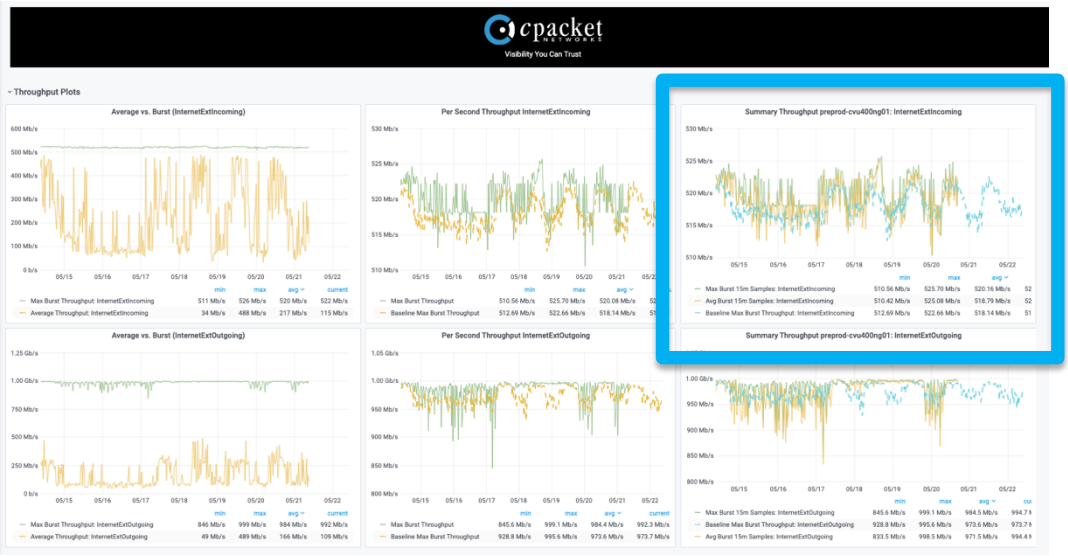


Diagram 2 – Network Throughput Average Burst, Max Burst, and Baseline Max Burst

In summary, the cPacket Two-Tier network monitoring and brokering architecture enables the following three key use cases and beyond:

- **Cost-effective, High Performance, Low-Latency Monitoring:** analyzing by link and port for high-speed core networks enables performance monitoring, PCAP storage, TCP analytics, microburst, predictive baselining, network health, and alerting.
- **Efficient Tool Utilization:** by monitoring and analyzing which security or performance tools connected to the packet broker are reaching their maximum capacity, timely tool upgrades can be planned, avoiding expensive downtimes and maximizing the ROI.
- **Application Dependency Monitoring:** by analyzing which applications are contributing to the congestion and reaching peak performance, either application or the network can be optimized for the best performance, increasing business continuity, and reducing MTTR.

Call to Action

Want to see the cPacket Two-Tier monitoring and brokering architecture in action? Request a product demo today.

About cPacket Networks

cPacket Networks enables IT through network-aware application performance and security assurance across the distributed hybrid environment. Our AIOps-ready single-pane-of-glass analytics provide the deep network visibility required for today's complex IT environments. With cPacket, you can efficiently manage, secure, and future-proof your network - enabling digital transformation. cPacket solutions are fully reliable, tightly integrated, and consistently simple. cPacket enables organizations around the world to keep their business running. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased security, reduced complexity, and increased operational efficiency. Learn more at www.cpacket.com