#225101
January 2025
Commissioned by
cPacket Networks

cPacket cStor® 200S Packet Capture & Analytics Observability Node

Ethernet Capture-to-Disk (CTD) Evaluation

Executive Summary

High-speed packet capture-to-disk (CTD) and observability is an essential requirement in many of today's most demanding environments including financial services (e.g., high-frequency trading), healthcare, and government. cPacket Networks provides this observability by delivering high-performance CTD solutions that can reliably keep up with 100GbE networks.

cPacket Networks commissioned Tolly to evaluate the CTD performance of its cPacket cStor 200S Packet Capture & Analytics Observability Node. All testing was run using 100GbE interfaces and focused on demonstrating performance with single and dual 100GbE interfaces active, with analytics enabled and analytics disabled, and demonstrating real-time search and download of specific captured traffic while capture was in progress.

The cPacket cStor 200S 220TB solution was able to execute all tasks without packet loss. Table 1 summarizes the performance tests.

Test Highlights

cPacket cStor 200S demonstrated:

1 CTD at 200 Gbps with analytics enabled or disabled

2 Search and download of full, raw packets in PCAP format while capturing at 200 Gbps with no packet loss during test with analytics enabled

3 CTD using self-encrypting drives with no degradation

4 CTD with Analytics enabled or disabled has the same performance

cPacket cStor 200S Network Capture-to-Disk with Zero Packet Loss
IMIX Traffic Streams (as generated by Ixia IxExplorer)

Network Interfaces	Traffic Load	Unique IP Endpoints	Unique Flows	Capture to Disk: Sustained Rate	Analytics Status	Search and Download
2x 100GbE	200 Gbps	20,000	20,000	200Gbps (66.9 million PPS)	Enabled	Yes
1x 100GbE	100 Gbps	20,000	20,000	100Gbps (33.4 million PPS)	Enabled	Yes
2x 100GbE	200 Gbps	10,000,000	10,000,000	200Gbps (66.9 million PPS)	Disabled	N/A
1x 100GbE	100 Gbps	10,000,000	10,000,000	100Gbps (33.4 million PPS)	Disabled	N/A

Note: 220TB, 4RU unit tested with self-encrypting drives. 100 percent capture of entire packet, no slicing or filtering. Average packet size was approximately 400 bytes. Capture rates reflect Ixia transmit rates with confirmed zero packet loss on cStor 200S unit. Sustained capture tests run for 20+ minutes. Because of inter-frame gaps and the IMIX traffic profile, 94.6Gbps is considered line-rate for a single 100GbE link and 189Gbps for 2 x 100GbE links. All tests run using cStor 200S v24.1.5.

Source: Tolly, December 2024

Table 1

Executive Summary (cont'd)

Performance with Analytics Enabled

The cPacket cStor 200S system demonstrated linear scalability capturing traffic with 20,000 unique IP addresses at 94.6 Gbps with analytics enabled using a single 100GbE interface and 189 Gbps using two 100GbE interfaces simultaneously with zero packet loss.

Performance with Analytics Disabled

The cPacket cStor 200S system again demonstrated linear scalability capturing traffic with 10 million unique IP addresses at 94.6 Gbps with analytics disabled using a single 100GbE interface and 189 Gbps using two 100GbE interfaces simultaneously with zero packet loss.

Packet Search and Download During Capture

Engineers were able to search for, and then download, a specific set of packets while the cStor 200S, with analytics enabled, captured traffic at sustained line rate with no packet loss.

Data At Rest Encryption

For this test, the cStor 200S was outfitted with self-encrypting drives (SED) for data-at-rest encryption with no performance degradation in any of the scenarios.

Detailed Test Results

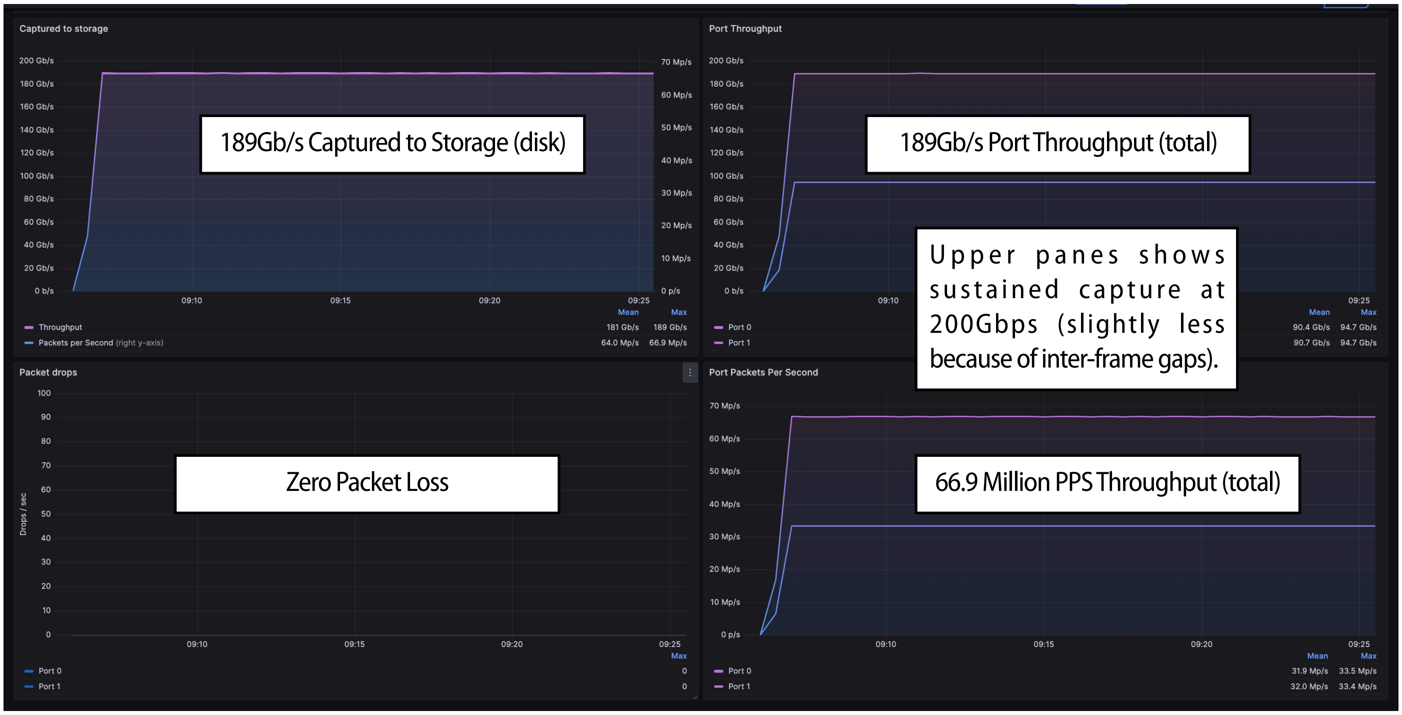
All tests were conducted using IPv4 TCP traffic, using the Ixia IMIX traffic profile, with either 20,000 or 10 million IP endpoint addresses across the flows. 20,000 addresses were used for the tests with analytics enabled. 10 million addresses were used for the tests with analytics disabled.

Performance with Analytics Enabled

Tests were run using either one 100GbE or two 100GbE network interfaces. As noted, results were linear with interfaces capturing to disk at line rate in both tests.

cPacket cStor 200S 2 x 100GbE Network Capture-to-Disk with Zero Packet Loss

Example Dashboard Display During Test Run



	Mean	Max
Throughput	181 Gb/s	189 Gb/s
Packets per Second (right y-axis)	64.0 Mp/s	66.9 Mp/s

	Mean	Max
Port 0	90.4 Gb/s	94.7 Gb/s
Port 1	90.7 Gb/s	94.7 Gb/s

	Max
Port 0	0
Port 1	0

	Mean	Max
Port 0	31.9 Mp/s	33.5 Mp/s
Port 1	32.0 Mp/s	33.4 Mp/s

189Gb/s Captured to Storage (disk)

189Gb/s Port Throughput (total)

Upper panes shows sustained capture at 200Gbps (slightly less because of inter-frame gaps).

Zero Packet Loss

66.9 Million PPS Throughput (total)

Note: Because of inter-frame gaps and the IMIX traffic profile, 94.6Gbps is considered line-rate for a single 100GbE link and 189Gbps for 2 x 100GbE links.

Source: Tolly, December 2024

Figure 1

With one 100GbE interface the CTD rate was 94.6 Gbps (33.4 million PPS). With two 100GbE interfaces the CTD rate was 189 Gbps (66.9) million PPS). See Table 1 and Figure 1.

To view the analytics one needs to use cPacket cClear via the user interface or the API. This is a separately licensed product.

Figure 2 shows a typical cClear analytics screen, this one illustrating the per-VLAN throughput.

Performance with Analytics Disabled

Tests were again run using either one 100GbE or two 100GbE network interfaces. As with the prior two tests, results were linear with interfaces capturing to disk at line rate in both tests.

With one 100GbE interface the CTD rate was 94.6 Gbps (33.4 million PPS). With two 100GbE interfaces the CTD rate was 189 Gbps (66.9 million PPS). See Table 1.

Packet Search and Download During Capture

While a capture is in progress, the user might need to download captured packets, for example, to begin a detailed investigation of a security incident from a given point in time using a small subset of network traffic.

This test was run as part of the "analytics enabled," one 100GbE interface test with a full load on the system. At about the 10-minute mark, a low-rate stream of packets with unique IP addresses were added into the traffic mix. These packets were then used as the target for the search and download task.

1,000 packets were inserted, and successfully located via search and download out of 40,140 million total packets based on searching over a 10 minute window with 66.9 Mpps traffic rate.

Search and download did not impact CTD performance.

cPacket Networks

cStor 200S Packet Capture & Analytics Observability Node

Tolly Certified

Capture-to-Disk Performance

Tested December 2024

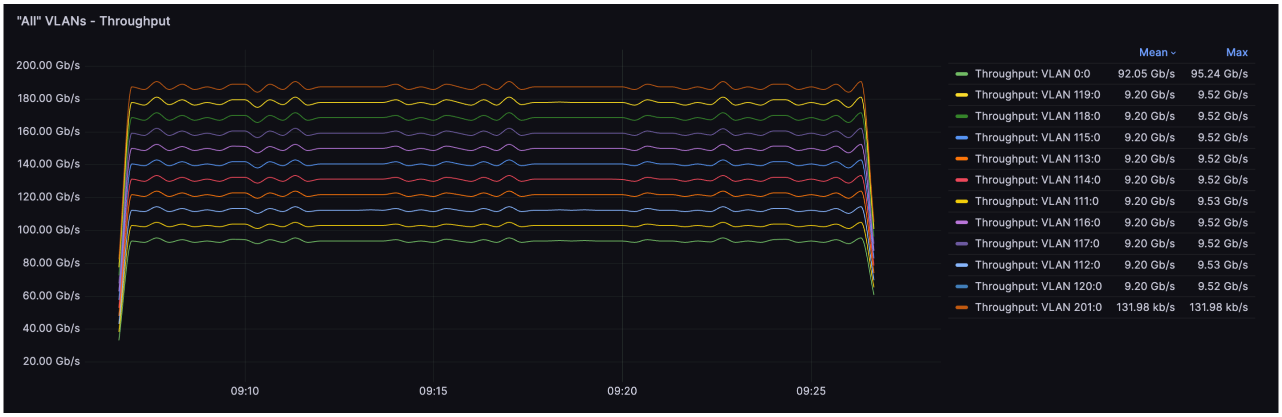
See Figure 3, on the next page, for a screenshot of the download task and the downloaded data opened in Wireshark network analyzer to confirm that the packets matched the search parameters.

Test Setup & Methodology

The test bed consisted of the cPacket Networks cStor 200S solution connected

cPacket cClear Analytics System

Example Display Showing Traffic Statistics for VLANs



	Mean ⌄	Max
Throughput: VLAN 0:0	92.05 Gb/s	95.24 Gb/s
Throughput: VLAN 119:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 118:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 115:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 113:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 114:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 111:0	9.20 Gb/s	9.53 Gb/s
Throughput: VLAN 116:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 117:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 112:0	9.20 Gb/s	9.53 Gb/s
Throughput: VLAN 120:0	9.20 Gb/s	9.52 Gb/s
Throughput: VLAN 201:0	131.98 kb/s	131.98 kb/s

Source: Tolly, December 2024

Figure 2

to an Ixia Networks (Keysight Technologies) traffic generator.

The Ixia SGS2 chassis platform hardware was used along with the Ixia IxExplorer. The ports of the Ixia hardware were directly connected to the ports of the system under test.

The cPacket cStor 200S was tested in its 4U, 220TB configuration. The cStor 200S system was running version 24.1.5 build 2391. The cClear system ran software version 24.2.0 build 2319.

IxExplorer was set to the appropriate number of IP endpoints and flows (either 20,000 or 10,000,000) for a given test along with the traffic rate.

The IMIX traffic profile was used for all tests. This resulted in an average frame size of ~400 bytes.

Capture/Write Data Tests

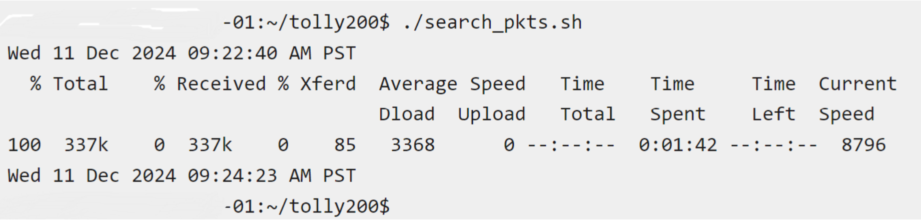
All tests were run using the same procedure. Traffic was generated via two network ports of the Ixia system and delivered to the two network ports of cStor 200S under test. No taps or packet brokers were used in the test.

During the test, the cStor dashboard was monitored. Each test was run for a minimum of 20 minutes. At the end of each test, engineers calculated the total packets generated by the Ixia system and compared that count to the capture count of the cStor. Zero packet loss was confirmed by the counters on the cStor.

Analytics, Download and Search Tests

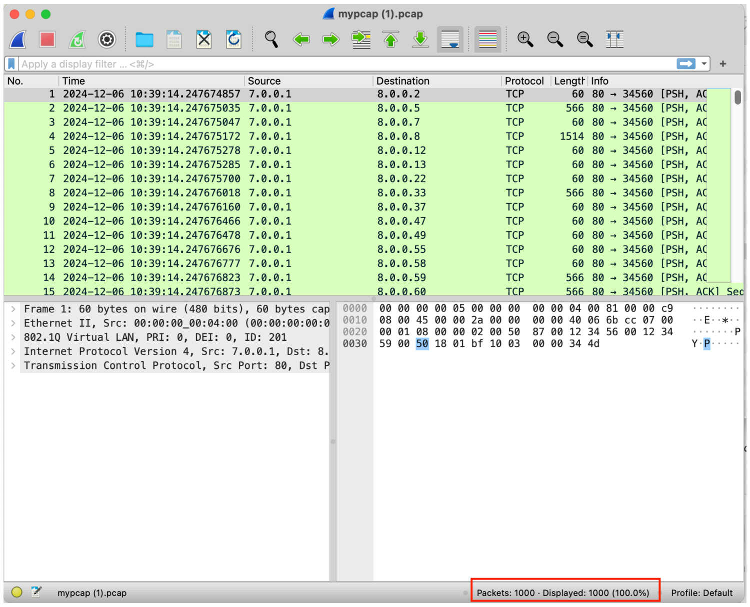
These tests are described in the Detailed Test Results section to provide better context to the reader.

cPacket Download Task & Review in Network Analyzer



Task to run the download of search results packets

```
                 -01:~/tolly200$ ./search_pkts.sh
Wed 11 Dec 2024 09:22:40 AM PST
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  337k    0  337k    0    85   3368      0 --:--:--  0:01:42 --:--:--  8796
Wed 11 Dec 2024 09:24:23 AM PST
                 -01:~/tolly200$
```



```
No.  Time                           Source    Destination  Protocol Length Info
   1 2024-12-06 10:39:14.247674857 7.0.0.1   8.0.0.2      TCP        60 80 → 34560 [PSH, AC
   2 2024-12-06 10:39:14.247675035 7.0.0.1   8.0.0.5      TCP       566 80 → 34560 [PSH, AC
   3 2024-12-06 10:39:14.247675047 7.0.0.1   8.0.0.7      TCP        60 80 → 34560 [PSH, AC
   4 2024-12-06 10:39:14.247675172 7.0.0.1   8.0.0.8      TCP      1514 80 → 34560 [PSH, AC
   5 2024-12-06 10:39:14.247675278 7.0.0.1   8.0.0.12     TCP        60 80 → 34560 [PSH, AC
   6 2024-12-06 10:39:14.247675285 7.0.0.1   8.0.0.13     TCP        60 80 → 34560 [PSH, AC
   7 2024-12-06 10:39:14.247675700 7.0.0.1   8.0.0.22     TCP        60 80 → 34560 [PSH, AC
   8 2024-12-06 10:39:14.247676018 7.0.0.1   8.0.0.33     TCP       566 80 → 34560 [PSH, AC
   9 2024-12-06 10:39:14.247676160 7.0.0.1   8.0.0.37     TCP        60 80 → 34560 [PSH, AC
  10 2024-12-06 10:39:14.247676466 7.0.0.1   8.0.0.47     TCP        60 80 → 34560 [PSH, AC
  11 2024-12-06 10:39:14.247676478 7.0.0.1   8.0.0.49     TCP        60 80 → 34560 [PSH, AC
  12 2024-12-06 10:39:14.247676676 7.0.0.1   8.0.0.55     TCP        60 80 → 34560 [PSH, AC
  13 2024-12-06 10:39:14.247676777 7.0.0.1   8.0.0.58     TCP        60 80 → 34560 [PSH, AC
  14 2024-12-06 10:39:14.247676823 7.0.0.1   8.0.0.59     TCP       566 80 → 34560 [PSH, AC
  15 2024-12-06 10:39:14.247676873 7.0.0.1   8.0.0.60     TCP       566 80 → 34560 [PSH, ACK] Sec
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes cap
> Ethernet II, Src: 00:00:00_00:04:00 (00:00:00:00:0
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 201
> Internet Protocol Version 4, Src: 7.0.0.1, Dst: 8.
> Transmission Control Protocol, Src Port: 80, Dst P
```

```
0000  00 00 00 00 05 00 00 00  00 00 04 00 81 00 00 c9   ········
0010  08 00 45 00 00 2a 00 00  00 00 40 06 6b cc 07 00   ··E··*··
0020  00 01 08 00 00 02 00 50  87 00 12 34 56 00 12 34   ·······P
0030  59 00 50 18 01 bf 10 03  00 00 34 4d               Y·P·····
```

mypcap (1).pcap Packets: 1000 · Displayed: 1000 (100.0%) Profile: Default

Downloaded file in PCAP format viewed directly in Wireshark. See bottom right that shows all 1,000 test packets captured.

Source: Tolly, December 2024

Figure 3

About Tolly

The Tolly Group companies have been delivering world-class IT services for over 35 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at *sales@tolly.com*, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.