TEST REPORT
Tolly.

#223119
April 2023
Commissioned by
cPacket Networks

cPacket cStor® 100S Packet Capture & Analysis Observability Node

Ethernet Capture-to-Disk (CTD) Evaluation

Executive Summary

Network accountability requires network observability. Whether the focus is reducing service outages, proving compliance, isolating security threats, or accelerating incident response, it is essential to be able to store and replay network traffic. cPacket Networks provides this observability by delivering a high-performance capture-to-disk (CTD) solution that can reliably keep up with today's 100GbE networks.

cPacket Networks commissioned Tolly to evaluate the capture-to-disk performance of its cPacket cStor 100S Packet Capture & Analysis Observability Node. Tests encompassed: 1) Baseline performance, 2) Performance with analytics enabled, 3) Packet download during capture, and 4) Packet search and download during capture. Tests were run on both the base 288 TB 4U system alone and then augmented by the 4RU cPacket extensible storage (CES) system for a total capacity of 2 PB and with both 40/100GbE network interfaces.

The cPacket cStor 100S solution was able to execute all tasks without degradation or packet loss. Table 1 summarizes the performance tests.

Test Highlights

cPacket cStor 100S demonstrated:

1 CTD at speeds of 40 Gbps, 80 Gbps, and 100 Gbps up to 33.4 million packets per second

2 CTD at 60.5 Gbps with analytics on

3 Reliably download raw packets in PCAP format while capturing at 100 Gbps with no packet loss

4 Search and download capability in PCAP format while the unit is capturing at 95Gbps with no packet loss

cPacket cStor 100S 40/100GbE Network Capture-to-Disk with Zero Packet Loss
IMIX Traffic Streams (as generated by Ixia IxExplorer 8.5)

cStor 100S Solution	Network Interfaces	Traffic Load	Unique IP Endpoints	Unique Flows	Capture to Disk: Maximum Sustained Rate	Analytics Status
288 TB (4RU)	2x 40GbE	40 Gbps	10,000,000	10,000,000	40 Gbps (13.4 million PPS)	Off
	2x 100GbE	60.5 Gbps	10,000,000	10,000,000	60.5 Gbps (20.2 million PPS)	Off
2 PB (8RU)	2x 40GbE	40 Gbps	10,000,000	10,000,000	40 Gbps (13.4 million PPS)	Off
	2x 100GbE	60.5 Gbps	20,000	20,000	60.5 Gbps (20.2 million PPS)	Off & On
	2x 100GbE	80 Gbps	20,000	20,000	80 Gbps (26.7 million PPS)	Off
	2x 100GbE	100 Gbps	20,000	20,000	100 Gbps (33.4 million PPS)	Off
	2x 100GbE	100 Gbps	10,000,000	10,000,000	100 Gbps (33.4 million PPS)	Off

Note: 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 100S unit. Sustained capture tests run for 20+ minutes. All tests run using cStor 100S v23.1.1.
Source: Tolly, April 2023

Table 1

Executive Summary (cont'd)

Baseline Performance

The cPacket cStor 100S 2 PB 8 RU system (base system plus CES) with analytics disabled can CTD (Capture to Disk) at sustained 100 Gbps (33 million PPS) with no packet loss.

The cPacket cStor 100S 288 TB 4 RU system with analytics disabled can CTD at sustained 60.5 Gbps with no packet loss.

Performance with Analytics Enabled

The cPacket cStor 100S 2 PB 8 RU system with analytics on can CTD at sustained 60.5 Gbps (20.2 million PPS) with no packet loss.

Packet Download During Capture

The cStor 100S 288 TB 4 RU system with analytics off was able to download packets and CTD at sustained 60.5 Gbps (20.2 million PPS) with no packet loss.

The cStor 100S 2 PB 8 RU system with analytics off was able to download packets and CTD at sustained 100 Gbps (33.4 million PPS) with no packet loss.

Packet Search and Download During Capture

Engineers were able to search for, and then download, a specific set of packets while cStor 100S 2 PB 8 RU with analytics CTD at sustained 95 Gbps with no packet loss.

Data At Rest Encryption

While beyond the scope of this test, cPacket notes that the cStor 100S can be installed with self-encrypting drives (SED) for data-at-rest encryption with no performance degradation in any of the above scenarios.

Detailed Test Results

All tests were conducted using a combination of real-world HTTP (TCP) traffic with between 20,000 and 10 million IP endpoint addresses across the flows.

Baseline Performance

Baseline tests were used to establish sustained capture rates for both the core and expanded cStor 100S units. Ixia IxExplorer outfitted with two ports was used to generate all traffic. For additional details, see Test Setup & Methodology.

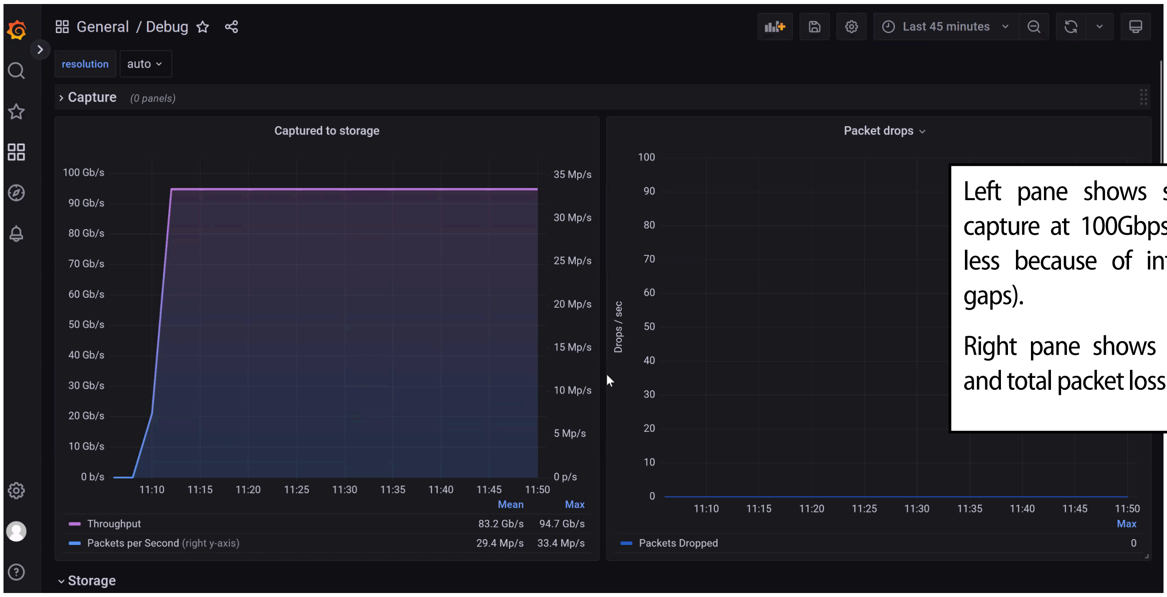
Tests were run using either 2x 40GbE or 2 x 100GbE network interfaces. Depending on the specific scenario, the unique number of IP endpoints and IP flows was either 20,000 or 10,000,000.

For the 2x 40GbE tests, sustained capture of 40 Gbps was tested. For the 2x 100GbE tests, sustained capture was tested at 60.5, 80, and 100 Gbps.

In all scenarios, the tests were 100% successful with CTD at the specified rate of 40/60.5/80/100 Gbps with zero packet loss. As noted, see Table 1. Figure 1, below, shows the dashboard screen after running 100 Gbps capture for close to 30 minutes. The left pane shows that all traffic was captured while the right pane shows zero packet loss

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

Example Dashboard Display



Left pane shows sustained capture at 100Gbps (slightly less because of inter-frame gaps).

Right pane shows real-time and total packet loss of zero.

Source: Tolly, April 2023

Figure 1

throughout the test run. Dashboard statistics for all of the other runs showed the same relative results based on traffic load.

Performance with Analytics Enabled

cPacket Networks offers an optional analytics mode for additional information that can be made available for review while the capture is in progress.

Tolly confirmed that the cStor 100S 2 PB solution with 2x 100GbE capturing to disk at the sustained rate of 60.5 Gbps could run with analytics enabled without any packet loss.

To view these 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. On this screen, the user is shown detailed statistics of the various VLANs found in the traffic stream. Information includes: maximum, average, and total traffic, flows, packets, fragment count, MTU, and more.

Packet Download During Capture

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

As noted earlier, engineers were able to download 100MB and 1GB files from the base unit while running CTD at 60.5 Gbps with zero packet loss. The same tests were performed, again without packet loss, on the larger system with a sustained capture rate of 95 Gbps.

Packet download was rapid. For example, the download of 100MB required only 28 seconds. cStor downloads packets in the industry-standard PCAP format with nanosecond-precision timestamps. Engineers opened the downloaded file using the the open-source Wireshark network analyzer. See Figure 3, on the next page, for a screenshot of the download task and the downloaded data opened in Wireshark.

cPacket Networks

cStor 100S Packet Capture & Analysis Observability Node

Tolly Certified

Capture-to-Disk Performance

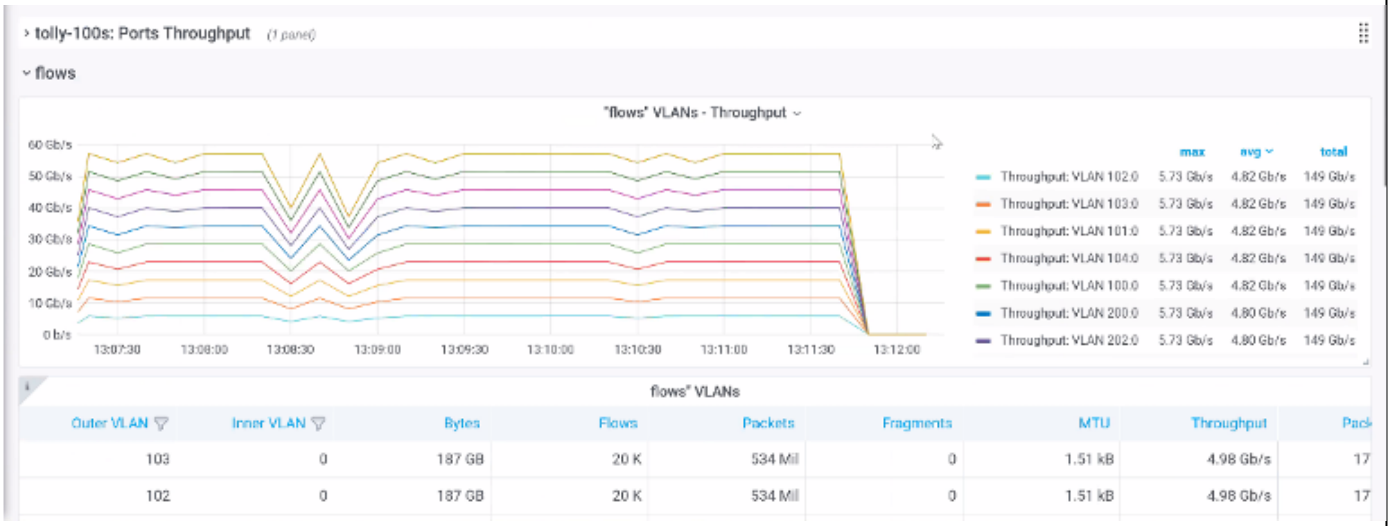
Tested April 2023

Packet Download and Search During Capture

Users might need to search for packets from a given IP address, again, while capture is in progress. To run this test, a 95Gbps load was placed on the cStor. After about 15 minutes, 1,000 packets with a specific IP address were transmitted into the stream. This test

cPacket cClear Analysis System

Example Display Showing Traffic Statistics for VLANs



	max	avg ˅	total
Throughput: VLAN 102:0	5.73 Gb/s	4.82 Gb/s	149 Gb/s
Throughput: VLAN 103:0	5.73 Gb/s	4.82 Gb/s	149 Gb/s
Throughput: VLAN 101:0	5.73 Gb/s	4.82 Gb/s	149 Gb/s
Throughput: VLAN 104:0	5.73 Gb/s	4.82 Gb/s	149 Gb/s
Throughput: VLAN 100:0	5.73 Gb/s	4.82 Gb/s	149 Gb/s
Throughput: VLAN 200:0	5.73 Gb/s	4.80 Gb/s	149 Gb/s
Throughput: VLAN 202:0	5.73 Gb/s	4.80 Gb/s	149 Gb/s

flows" VLANs

Outer VLAN	Inner VLAN	Bytes	Flows	Packets	Fragments	MTU	Throughput	Pack
103	0	187 GB	20 K	534 Mil	0	1.51 kB	4.98 Gb/s	17
102	0	187 GB	20 K	534 Mil	0	1.51 kB	4.98 Gb/s	17

Source: Tolly, April 2023

Figure 2

specified a start-time and end-time to bracket the search. The test was run twice, once with a 5-minute search window and again with a 10-minute window. The capture stream was growing to 150+ billion packets during the search.

Different IP addresses were inserted for each run. The packets being searched for were inserted near the end of the search window.

In both cases, the search was quite fast. For the test of the 5-minute window, the packets were discovered and downloaded after 11 minutes and 25 seconds. For the test of the 10-minute window, the packets were discovered and downloaded after 22 minutes and 47 seconds. Engineers viewed the downloaded packets in the Wireshark network analyzer to confirm that the packets matched the search parameters.

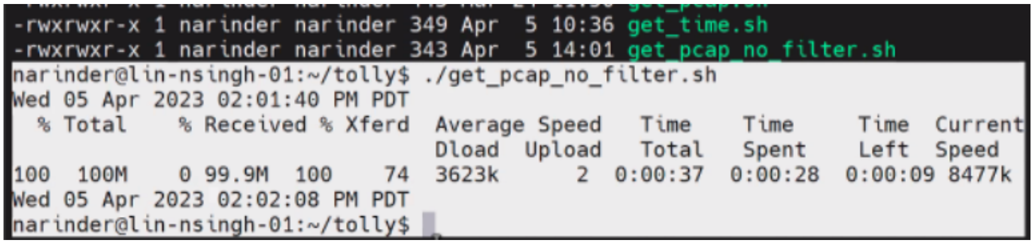
Test Setup & Methodology

The test bed consisted of the cPacket Networks cStor 100S solution connected to an Ixia Networks (Keysight Technologies) traffic generator.

The Ixia SGS2 chassis platform hardware was used along with the Ixia IxExplorer. Two ports of the Ixia hardware were directly connected to the two ports of the system under test. For the 40GbE tests the appropriate transceivers were used.

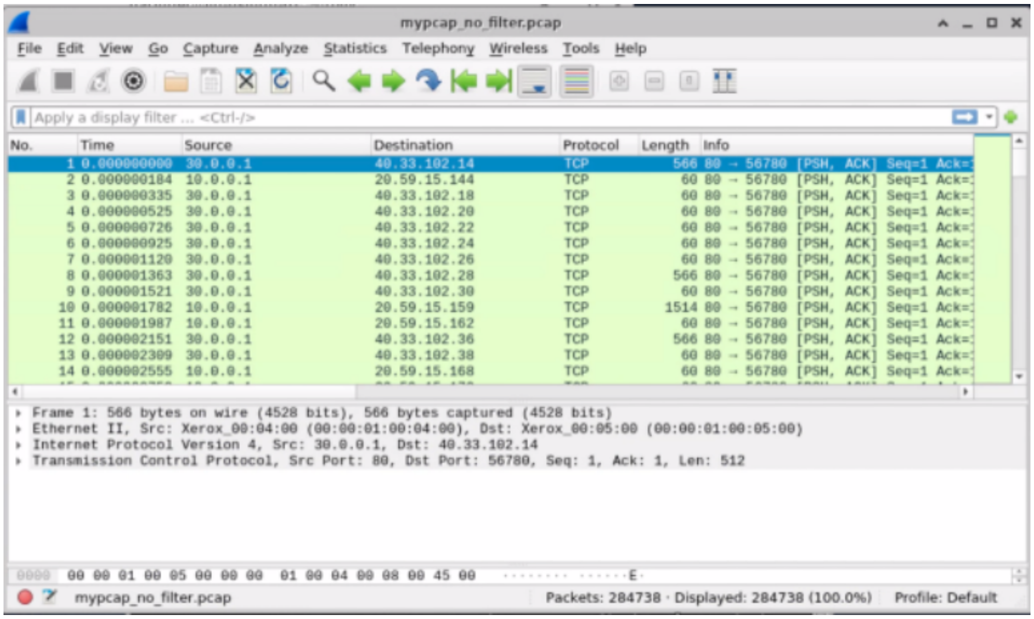
cPacket Download Task & Review in Network Analyzer

Task to run the download (Download size set in script.)



```
-rwxrwxr-x 1 narinder narinder 349 Apr  5 10:36 get_time.sh
-rwxrwxr-x 1 narinder narinder 343 Apr  5 14:01 get_pcap_no_filter.sh
narinder@lin-nsingh-01:~/tolly$ ./get_pcap_no_filter.sh
Wed 05 Apr 2023 02:01:40 PM PDT
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  100M    0 99.9M  100    74  3623k      2  0:00:37  0:00:28  0:00:09 8477k
Wed 05 Apr 2023 02:02:08 PM PDT
narinder@lin-nsingh-01:~/tolly$
```

Downloaded file in PCAP format viewed directly in Wireshark.



mypcap_no_filter.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time         Source      Destination     Protocol  Length Info
    1 0.000000000  30.0.0.1    40.33.102.14    TCP        566 80 → 56780 [PSH, ACK] Seq=1 Ack=
    2 0.000000184  10.0.0.1    20.59.15.144    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
    3 0.000000335  30.0.0.1    40.33.102.18    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
    4 0.000000525  30.0.0.1    40.33.102.20    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
    5 0.000000726  30.0.0.1    40.33.102.22    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
    6 0.000000925  30.0.0.1    40.33.102.24    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
    7 0.000001120  30.0.0.1    40.33.102.26    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
    8 0.000001363  30.0.0.1    40.33.102.28    TCP        566 80 → 56780 [PSH, ACK] Seq=1 Ack=
    9 0.000001521  30.0.0.1    40.33.102.30    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
   10 0.000001782  10.0.0.1    20.59.15.159    TCP       1514 80 → 56780 [PSH, ACK] Seq=1 Ack=
   11 0.000001987  10.0.0.1    20.59.15.162    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
   12 0.000002151  30.0.0.1    40.33.102.36    TCP        566 80 → 56780 [PSH, ACK] Seq=1 Ack=
   13 0.000002309  30.0.0.1    40.33.102.38    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=
   14 0.000002555  10.0.0.1    20.59.15.168    TCP         60 80 → 56780 [PSH, ACK] Seq=1 Ack=

▸ Frame 1: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits)
▸ Ethernet II, Src: Xerox_00:04:00 (00:00:01:00:04:00), Dst: Xerox_00:05:00 (00:00:01:00:05:00)
▸ Internet Protocol Version 4, Src: 30.0.0.1, Dst: 40.33.102.14
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 56780, Seq: 1, Ack: 1, Len: 512

0000  00 00 01 00 05 00 00 00  01 00 04 00 08 00 45 00   ········ ······E·

mypcap_no_filter.pcap          Packets: 284738 · Displayed: 284738 (100.0%)   Profile: Default
```

Source: Tolly, April 2023

Figure 3

The cPacket cStor 100S was tested in two disk storage configurations: 1) 288 TB, and 2) 2 PB. The two petabyte version is known as cPacket Extensible Storage or CES. For tests using the smaller configuration, the extra 100+ drives in the CES were taken offline. Tolly engineers confirmed that the CES drivers were online/offline as appropriate. The cStor 100S system was running version 23.1.1.

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 results in an average frame size of ~400 bytes. Each Ixia port generated half of the overall traffic for each test.

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 100S under test. No taps or packet brokers were used in the test.

In each test, the traffic generated was above the claimed performance level for each solution.

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. To validate that the lost packet counters were operational, tests were run that generated some packet loss and Tolly engineers confirmed that the lost packet counter was incremented.

Analytics, Download and Search Tests

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

About Tolly

The Tolly Group companies have been delivering world-class IT services for over 30 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.

223119-db-1-wt-2023-05-14-VerH