T6 100GbE Crypto Offload Performance

Superior Throughput with Chelsio Crypto Offload Solution

Executive Summary

Chelsio's Terminator 6 (T6) Unified Wire ASIC enables concurrent secure communication and secure storage with support for integrated TLS/SSL/DTLS and inline cryptographic functions, leveraging the proprietary TCP/IP offload engine. Chelsio's full offload TLS/SSL/DTLS is uniquely capable of 100Gb line-rate performance. In addition, the accelerator can be used in a traditional co-processor Lookaside mode to accelerate TLS/SSL, IPsec, SMB 3.X crypto, data at rest encryption/decryption, and data-deduplication fingerprint computation.

This paper presents benchmark results of Co-processor mode with different SHA digest algorithms using the T6 adapters running at 100Gbps. The preliminary results provide a preview of the benefits of Chelsio's Crypto offload technology over regular NIC adapters, showing superior throughput. Chelsio's T6 solution delivers the highest performance for Crypto in Linux. The paper also presents throughput results in Inline TLS/SSL mode.

Overview

The Terminator 6 (T6) ASIC from Chelsio Communications, Inc., is a sixth generation, highly integrated, hyper-virtualized 1/10/25/40/50/100GbE controller with full offload support for a complete Unified Wire solution. T6 enables a unified wire for LAN, SAN and cluster applications, built upon a high bandwidth and low latency architecture, along with a complete set of storage and cluster protocols operating over Ethernet (iSCSI, SMBD, iWARP, NVMe over Fabrics and FCoE). Unified Wire means having the ability to utilize all offload or non-offload protocols at the same time, over the same link, using the exact same firmware, host software and adapter. It scales to true 100 Gigabit line rate operation, from a single TCP connection to thousands of connections.

Support for integrated TLS/SSL, DTLS, IPsec and SMB 3.X crypto in the T6 adapters will enable tremendous differentiation for end products. With Inline Mode, the TLS/SSL processing happens in cut-through for both transmit and receive, as the rest of the TCP/IP processing and therefore adds minimal latency to the processing pipeline. T6 supports all the most popular AES, SHA1 and SHA2 digest algorithms with 100Gbps bandwidth and less than 2µs end-to-end latency. With Co-processor mode of operation, Crypto can be combined with the various offload capabilities of T6 to support secure operation always everywhere. The T6 can lower CAPEX and OPEX by offloading crypto to the NIC (all for the same price and power) rather than investing in a more powerful processor with crypto capabilities. Chelsio's adapter is benchmarked in Crypto offload mode and NIC mode, demonstrating the performance advantages and the benefits of its unique Crypto Offload technology at 100Gbps speed.

Test Results

Co-Processor mode with digest:

The following graphs compare OpenSSL speed in Co-processor (Hardware Offload) and Software (AES NI enabled) modes with different SHA digest algorithms. The I/O size used varies from 4KB to 32KB.

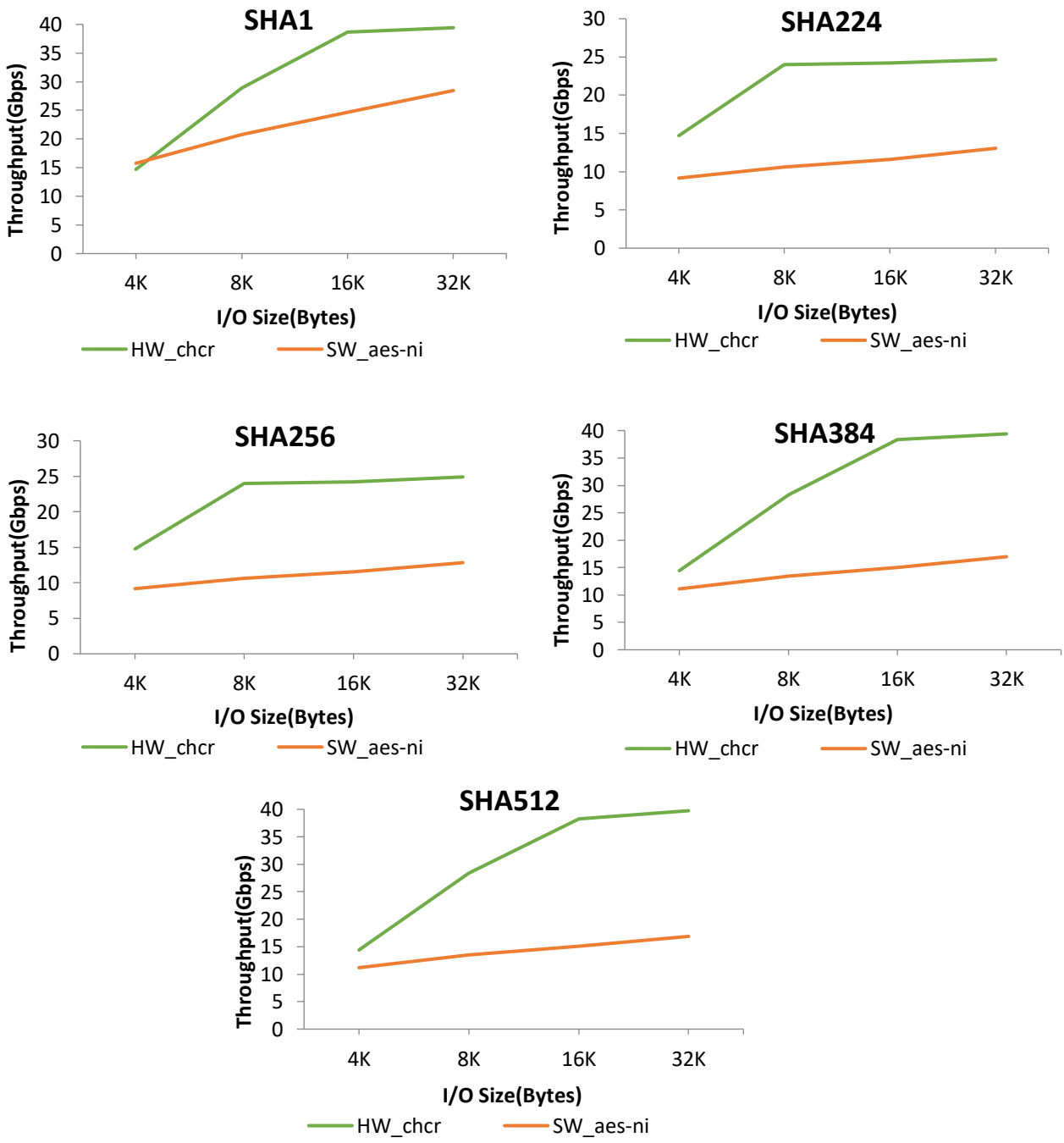

Figure 1 – Co-processor mode Throughput vs. I/O size

The above graphs show that the Co-processor mode throughput numbers are up to 2x that of standard NIC mode, indicative of a more efficient processing path.

Inline TLS/SSL mode:

The following table shows the inline OpenSSL Single port throughput numbers:

Inline TLS/SSL	Throughput (Gbps)
Transmit	91
Receive	77

Test Setup

Topology

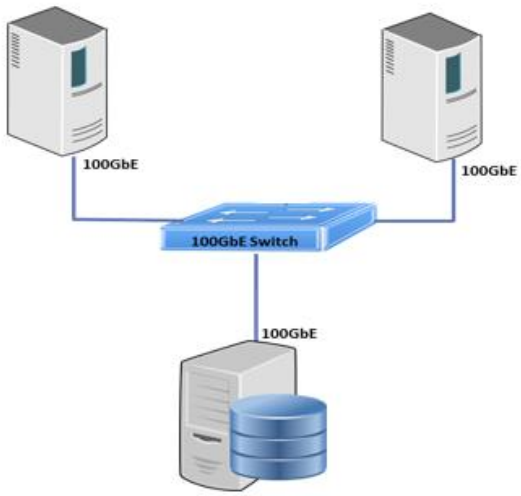

Figure 2 – Inline mode Setup

Network Configuration

Inline TLS/SSL mode:

The setup consists of 1 server and 2 client machines, connected via a 100GbE Switch. Each machine is configured with 2 Intel Xeon CPU E5-2687W v4 12-core processors @ 3.00GHz (HT disabled) and 128GB of RAM. Chelsio T62100-LP-CR adapter is installed in each system with RHEL 7.2 operating system (4.8 kernel). MTU of 9000B is used. Each client uses 6 connections to the Server.

Co-Processor mode with digest:

The setup consists of a standalone machine with 1 Intel Xeon CPU E5-1620 v4 4-core processor @ 3.5GHz (HT enabled) and 16GB of RAM. Chelsio T62100-LP-CR adapter is installed in the system with RHEL 7.2 operating system (4.8 kernel).

Commands Used

Co-Processor mode with digest:

```
[root@host]# ./openssl openssl speed -elapsed  -evp <sha suite> -multi 64
```

Inline TLS/SSL mode:

Server:

```
[root@host]#  ./openssl  s_server  -key  <server.key>  -cert  <server.crt>  -accept
<SSL port no> -cipher AES128-GCM-SHA256 -WWW &
```

Client:

```
[root@host]# ./openssl s_time -connect 192.168.1.144: <SSL port no> -www /1g -
time 200
```

Conclusion

Chelsio T6 100GbE adapters demonstrated unmatched Crypto performance in Co-processor (with different SHA digest algorithms) and Inline modes. These preliminary results will further improve with the ongoing performance tuning. T6 adapters are the only adapters that can offload a range of protocols including NVMe-oF, NIC, TOE, iSCSI, FCoE, iWARP RDMA and concurrently support TLS/SSL, DTLS, SMB 3.X crypto and IPsec. They enable concurrent secure communication and secure storage, all for the price and power of a typical NIC.

Related Links

The Chelsio Terminator 6 ASIC
T6 Crypto Offload
High Performance iSCSI at 100GbE
Introducing NVMe over 100GbE iWARP Fabrics
Windows SMB 3.1.1 Performance at 100Gbps