SOLUTION BRIEF
Intel® QuickAssist Technology

Scaling Acceleration Capacity from 5 to 50 Gbps and Beyond with Intel® QuickAssist Technology

Equipment manufacturers can dial in the right capacity by choosing from a family of Intel® chipsets or designing in multiple chipsets.

"Intel is making it easier to scale compression and cryptography capacity with the Intel® Platform for Communications Infrastructure that has built-in acceleration for common workloads . . . "

Highly Scalable Solution

Compression and cryptography are becoming check-off requirements for network equipment deployed in wireless, telecom, cloud, data centers, and enterprises. While there is a universal need to preserve network bandwidth and better protect traffic, the amount of processing required for these functions varies considerably among different network operators. This presents a challenge for equipment manufacturers who want to serve multiple market segments with cost-effective products that deliver the right level of performance.

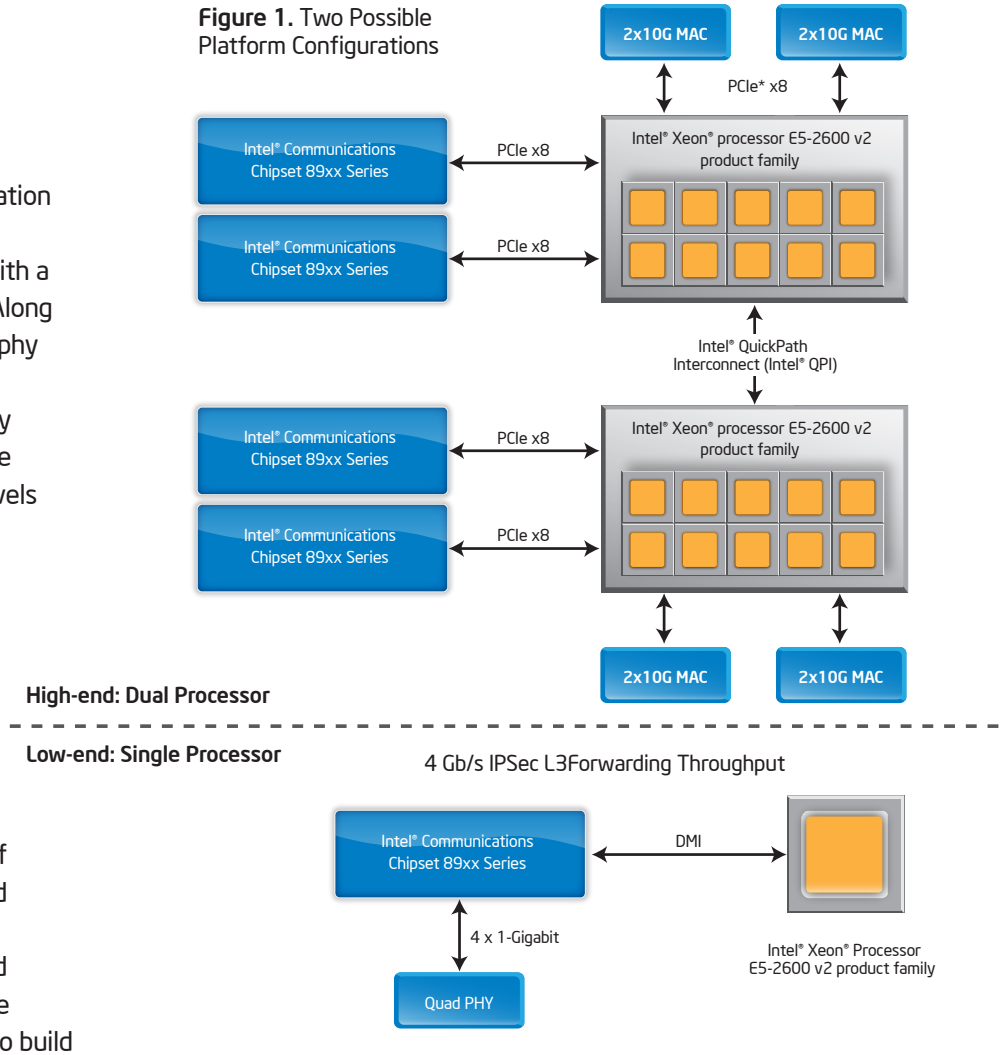
Intel is making it easier to scale compression and cryptography capacity with the Intel® Platform for Communications Infrastructure that has built-in acceleration for common workloads, including packet forwarding, bulk cryptography, and compression. These capabilities, available on commercial off-the-shelf (COTS) servers, are a more flexible alternative to purpose-built hardware. Performance throughput of approximately 255 million packets per second (MPPS) of L3 forwarding and 80 gigabits (Gbps) per second of IPsec acceleration[1,2] have been demonstrated on servers with dual Intel® Xeon® processor E5-2600 v2 product family series and Intel® Communications Chipset 89xx Series.

This solution brief discusses how to scale cryptographic and compression workloads on Intel® architecture, and is one in a series of five briefs describing how to maximize the benefits from Intel® QuickAssist Technology. Please see the Resources section for links to the series.

Platform Configuration Examples

Figure 1 illustrates a high-end configuration with dual, ten-core processors and four chipsets, and a low-end configuration with a single-core processor and one chipset. Along with scaling compression and cryptography capacity by adding chipsets, equipment manufacturers can fine-tune capacity by selecting from a family of pin-compatible Intel® chipsets that support different levels of workload acceleration.

Figure 1. Two Possible Platform Configurations



IPsec Workload Performance

Figure 2 shows the IPsec throughput of an Intel QuickAssist Technology-enabled system featuring a ten-core Intel® Xeon® processor E5-2680 v2 running the Wind River® Intelligent Network Platform®. The platform enables equipment providers to build high-performance, high-value products that accelerate, analyze, and secure network traffic and applications. It is an integrated and optimized software system, consisting of the critical run-time components and life cycle development tools needed to build intelligent network elements. Using the cryptographic acceleration from a single Intel® Communications Chipset 8950, the system sustained a throughput of nearly 40 Gbps while using as few as two processor cores. When a second Intel chipset was added, the throughput scaled linearly to nearly 80Gbps.

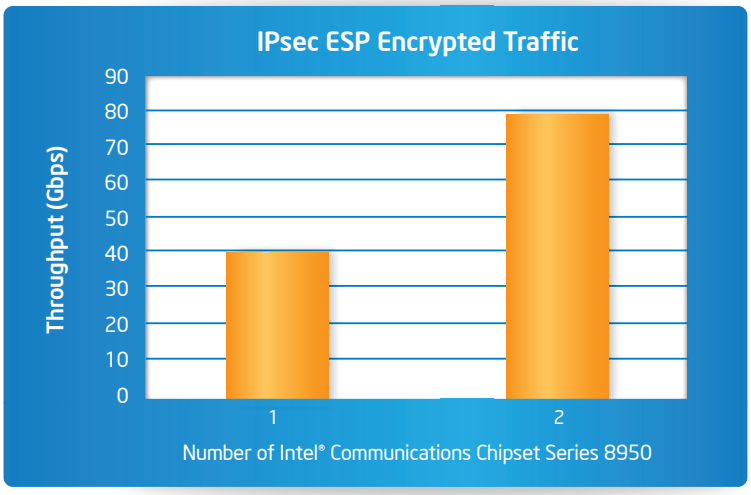


Figure 2. Scalable IPsec Performance

SSL Workload Performance

The Intel Communications Chipset 89xx Series has built-in cryptographic acceleration to speed up SSL/TLS workloads. It encrypts/decrypts SSL/TLS records, helps establish SSL/TLS connections by generating random numbers, and accelerates public key cryptographic algorithms such as RSA, DSA, Diffie-Hellman, ECDH, and ECDSA.

SSL/TLS record encryption/decryption is supported through the acceleration of all common SSL/TLS cipher suites used for ciphering and MAC digest generation and verification. Digest and ciphering operations can be performed in parallel, on the same record, in a single pass through the accelerator on the Intel Communications Chipset 89xx Series.

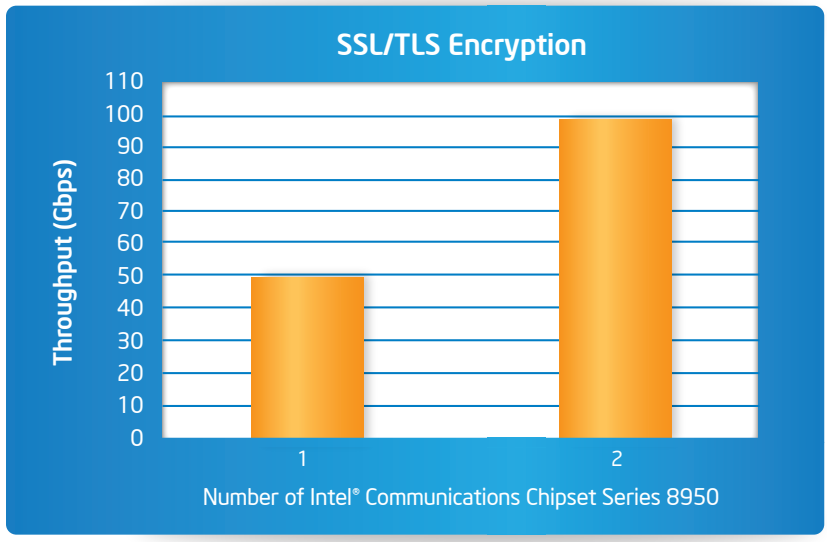


Figure 3. Scalable SSL/TLS Encryption Performance (AES128-CBC and SHA1-HMAC measured using OpenSSL* speed)

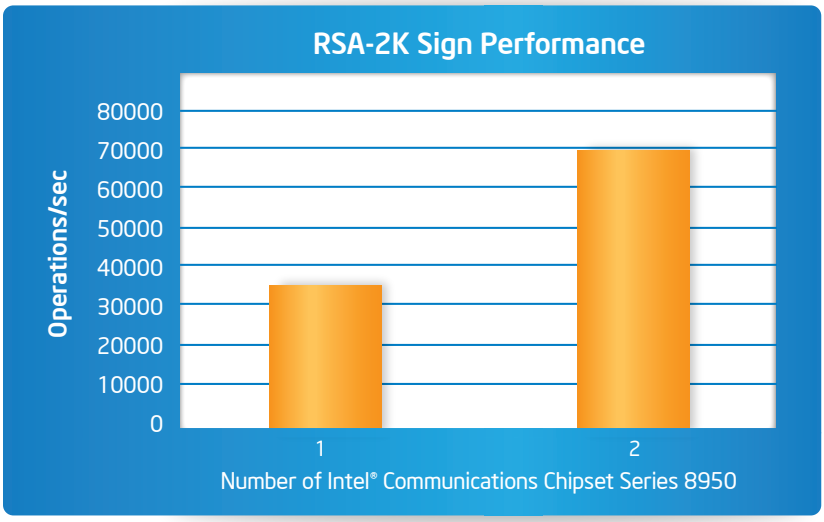


Figure 4. Scalable RSA-2K Sign Performance

Figure 3 shows one chipset supported an SSL/TLS encryption throughput rate of nearly 50 Gbps, and adding a second chipset doubled the performance.

Public key cryptographic performance was also measured, and one chipset delivered approximately 35 thousand RSA-2K operations per second, while two chipsets provided twice the performance (**Figure 4**).

Compression Workload Performance

Intel Communications Chipset 89xx Series performs lossless data compression and decompression using the LZ77 and LZS

algorithms. This acceleration functionality is available to applications via either an accelerated version of the popular zlib library or by directly accessing the Intel QuickAssist Technology API. **Figure 5** illustrates the accelerated zlib performance of a single Intel Communications Chipset 8950 Series operating on the Calgary Corpus* data set. This performance scales linearly as more chipsets are added to a platform.

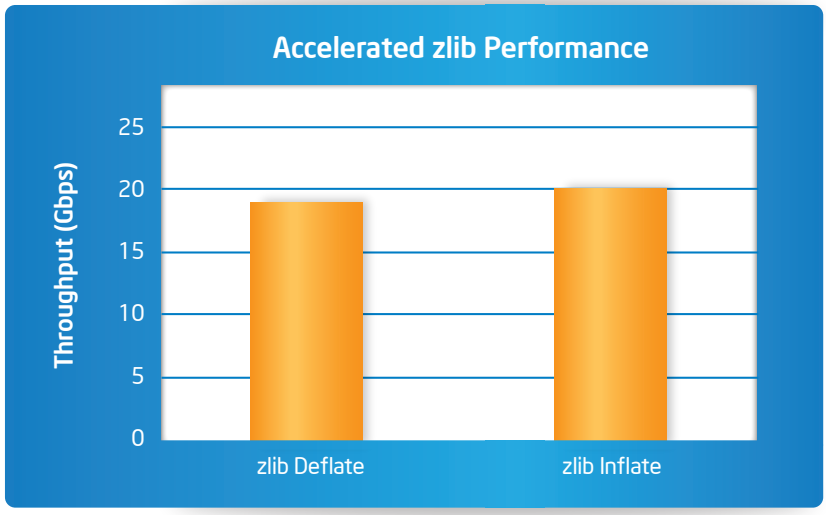


Figure 5. Accelerated zlib Performance for Compression and Decompression (Using a single Intel® Communications Chipset 8950)

Two Scalability Vectors

With Intel QuickAssist Technology, equipment manufacturers have two ways to linearly scale compression and cryptography performance – by choosing between chipset family members or by adding up to four chipsets to a dual-processor platform, as illustrated in **Table 1**. This flexibility enables manufacturers to meet multiple price-performance targets for different customer sets while using a common code base running on Intel architecture processors.

Table 1. Two Ways to Scale Capacity with Intel® QuickAssist Technology

SSL (Gbps)	Intel® Communications Chipset 89xx Series					
SKU	8900	8903	8910	8920	8925	8950
One Chipset	0	5G	10G	20G	25G	50G
Two Chipsets						100G
Three Chipsets						150G
Four Chipsets						200G

Resources

Solution Brief Series: Intel® QuickAssist Technology
Part 1: Integrated Cryptographic and Compression Accelerators on Intel® Architecture Platforms
Part 2: Bridging Open Source Applications and Intel® QuickAssist Technology Acceleration
Part 3: Accelerating OpenSSL* Using Intel® QuickAssist Technology
Part 4: Accelerating Hadoop* Applications Using Intel® QuickAssist Technology
Part 5: Scaling Acceleration Capacity from 5 to 50 Gbps Intel® QuickAssist Technology

Appendix A: Platform Configuration

Hardware Platform Configuration	
Processor	Dual socket Intel® Xeon® processor E5-2680 v2
Chipset	Intel® Communications Chipset 8950 (Intel® DH8950 PCH)
Memory	32GB DDR3 @ 1333MHz
Networking Card	Dual Port Intel® 82599ES 10 Gigabit Ethernet Controller
Operating System	Wind River* Linux* v5.0.1.6
Compiler	gcc v4.6.3

For more information About Intel QuickAssist Technology, visit
http://www.intel.com/content/www/us/en/io/quickassist-technology/quickassist-technology-developer.html

[1] Performance estimates are based on internal Intel analysis and are provided for informational purposes only.

[2] Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit http://www.intel.com/performance/resources/limits.htm

Printed in USA MS/VC/1113 Order No. 329878-001US