NA-360 Technical Announcement

Disclaimers

The information in this document has been carefully checked and is believed to be accurate. Axiomtek Co., Ltd. assumes no responsibility for any infringements of patents or other rights of third parties that may result from its use.

Axiomtek assumes no responsibility for any inaccuracies that may be contained in this document. Axiomtek makes no commitment to update or to keep current the information contained in this manual. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Axiomtek Co., Ltd.

All brand and product names are trademarks or registered trademarks of their respective companies. Please visit our web site for newest version of this Hardware Specification and for other information (like Product Info or drivers).

Trademarks Acknowledgments

AXIOMTEK is a trademark of Axiomtek Co., Ltd.
MS-DOS, and Windows 98/NT/2000/XP/7 are trademarks of Microsoft Corporation.
Intel is a registered trademark of Intel Corp.
Other brand names and trademarks are the properties and registered brands of their respective owners.

Enable Intel® QuickAssist Technology (QAT) on Network Appliance

ABSTRACT

Intel® QuickAssist Technology (QAT) makes it easier for developers to integrate embedded accelerators in their designs. Developers can use Intel® QuickAssist Technology to decrease development time by avoiding the need to develop proprietary acceleration layers for each new design, device, or appliance. Accelerate performance for demanding applications with specific hardware acceleration modules. QAT also support migration to designs using system-on-chip (SOC) and multi-core processors. Increase business flexibility with solutions that fit changing business requirements without being tied to a particular accelerator. Developers can easily migrate from one technology to another with minimum impact to applications by using an Accelerator Abstraction Layer (AAL).

Axiomtek Network Appliance Product Group (PG) has performed Intel® QAT technology in the latest network platform NA-360, the Crystal Forest Gladden platform. The test result shows comparison with/without running QuickAssist SDK of acceleration of packet PKE, and IPsec tunnel on strongSwan on the platform.

QuickAssist*® *Components:

- **Pre-boot Firmware**

  The Intel® Communications Chipset 89xx Series (PCH) pre-boot firmware (provided by an IBV) executes when the system is reset or powered up. It initializes and configures system memory, chipset functions, interrupts, console, devices, disk devices, integrated I/O controllers, PCI buses and devices, and additional application processors (AP) if present. IBV pre-boot firmware solutions are available to support both the legacy BIOS interface and the newer Unified Extensible Firmware Interface (UEFI).

- **Standard OS Drivers**

  These drivers (provided in a standard OS distribution) include support for standard peripherals on a traditional Intel® architecture platform such as USB, SATA, Ethernet* and so on. Intel provides a patch to the OS so that it recognizes the Device IDs (DIDs).

- **Acceleration Software Subsystem**

  A subsystem (provided by Intel) includes the software components that provide acceleration to applications running on the PCH. It contains the following:

  -- Services (Cryptographic, Data Compression)

  Including the firmware drives the various workload slices in the accelerator(s) and the associated Intel® architecture Service libraries that expose these workloads via APIs. The Service libraries use the Acceleration Driver Framework (ADF) to plug into the OS and gain access to the hardware to communicate with the firmware.

  -- Intel® QuickAssist Technology APIs

  The Intel® QuickAssist Technology APIs provide service level interfaces for customer applications or Ecosystem Middleware to access the accelerator(s) in the PCH.

  -- Acceleration Driver Framework (ADF)

  The Acceleration Driver Framework (ADF) includes infrastructure libraries that provide various services to the different software components of the acceleration drivers. The software framework is used to provide the acceleration services API to the application.

- **Open Source Frameworks**

  This layer includes open source stacks, such as the Linux Kernel Crypto framework, zlib, and OpenSSL. The software package works to integrate the Intel® QuickAssist Technology APIs with these stacks using patch layers. These open source stacks are not developed or provided by Intel.

- **Patch Layers**
  As described above, the PCH integrates with different OS stacks and Ecosystem Middleware using patch layers (translation layers). These patch layers may be developed by Intel or ecosystem vendors.

- **Customer Applications**
  Customer applications may connect to the Services directly via the Intel® QuickAssist Technology API or may connect though the supported open source frameworks and associated patches. Such applications can migrate to the PCH with little or no change provided that the Intel® QuickAssist Technology APIs are integrated with the OS stack or middleware used.

- **Logical Instances**
  A logical instance may be thought of as a channel to the hardware. A logical instance allows an address domain (that is, kernel space and individual user space processes) to configure the rings to be used by that address domain and to define the behavior of that ring.

- **Response Processing**
  Each logical instance may be configured to operate in one of two modes:
  -- Interrupt mode
  -- Polled mode

- **Operating System Support**
  The software package supports the Linux*, FreeBSD* and Windows* operating systems. The Acceleration driver is validated with the Linux operating system only. Details of the specific operating system versions supported depend on the release version. See the Release Notes for your release version for details on the specific operating system support provided in that release version.

- **OpenSSL Library Inclusion and Usage**
  The Intel® Communications Chipset 89xx Series software Linux* package is distributed with an OpenSSL library file. This library file has certain dependencies that will be met in most cases. In the event that these dependencies are not met, it may be necessary to build OpenSSL on the development platform and link any Intel® Communications Chipset 89xx Series software applications to the relevant OpenSSL library.

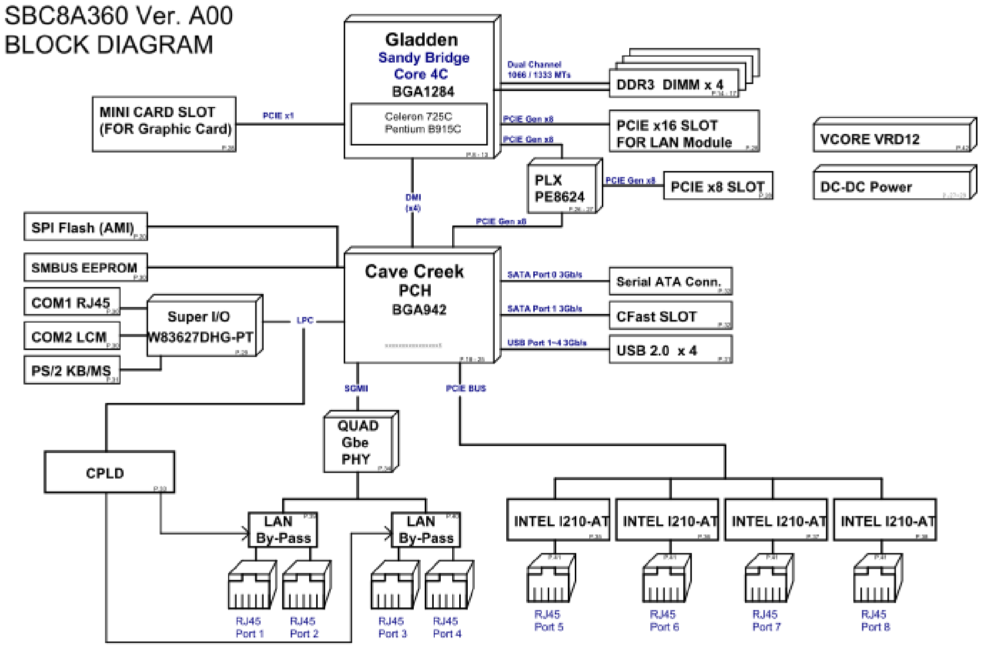


Figure 1

The Platform:

Axiomtek's NA-360 pairs an Intel® architecture processor Gladden, Pentium® Processor B915C (3MB Cache, 1.5GHz) with the Intel® Communications Chipset 8903C. Functionally, Intel® Communications Chipset 89xx Series can be most easily described as a Cave Creek Platform Controller Hub (PCH) that includes both standard PC interfaces (for example, PCI Express*, SATA, USB and so on) together with accelerator and I/O interfaces (for example, Intel® QuickAssist Accelerator and GigE). For I/O-optimized applications, Intel® Xeon® and Intel® Core™ Processors for Communications Infrastructure are paired with the Intel® Communications Chipset 89xx Series. Figure 1 is a block diagram of NA-360.

System Configuration:

- RAM: 2G DDR3 1333
- OS: Fedora 16, Kernel 3.1.0
- SDK: DH89xxCC.L.0.9.0-174.tar.gz
- Test Command: Insmod ./cpa_sample_code.ko runTest=63

The Test 1:

Run QuickAssist SDK on the NA-360 and compare packet performance: (1) encrypt with QAT device, and (2) encrypt without QAT device.

The result:

Crypt/Encrypt: AES128-CBC

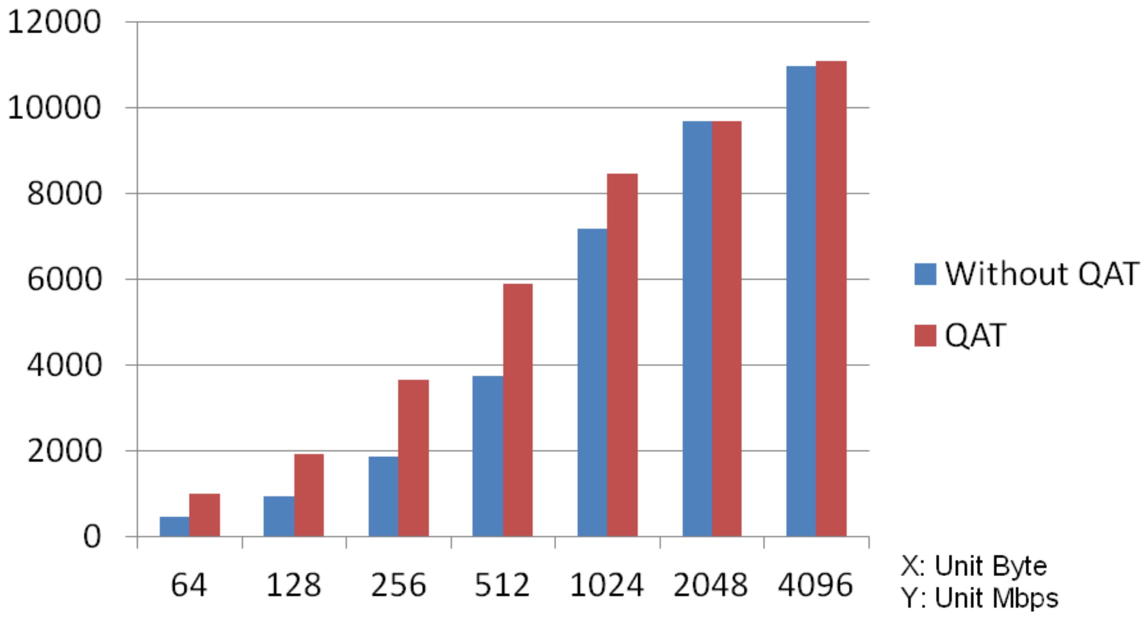


Figure 2

Crypt/Encrypt: AES256-CBC

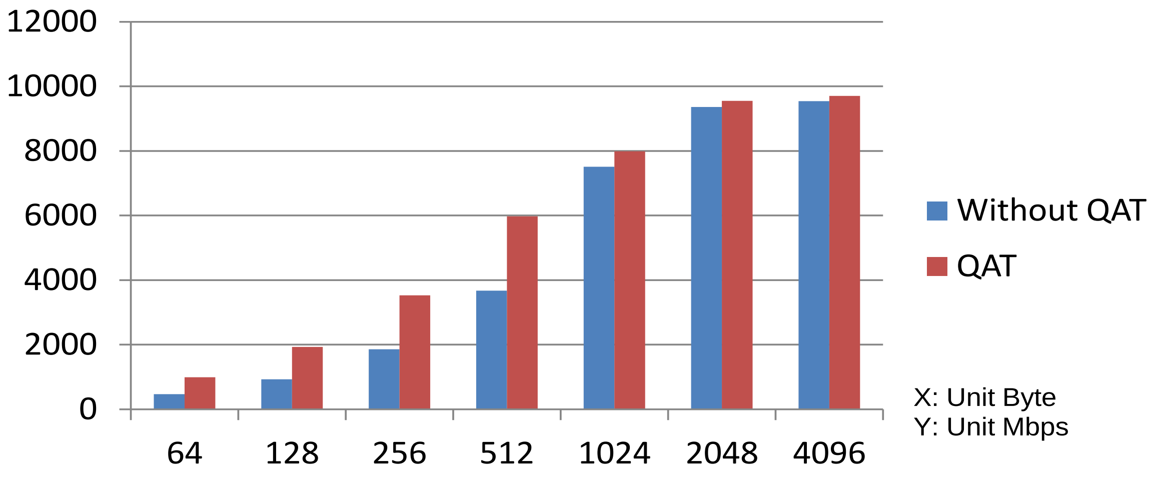


Figure 3

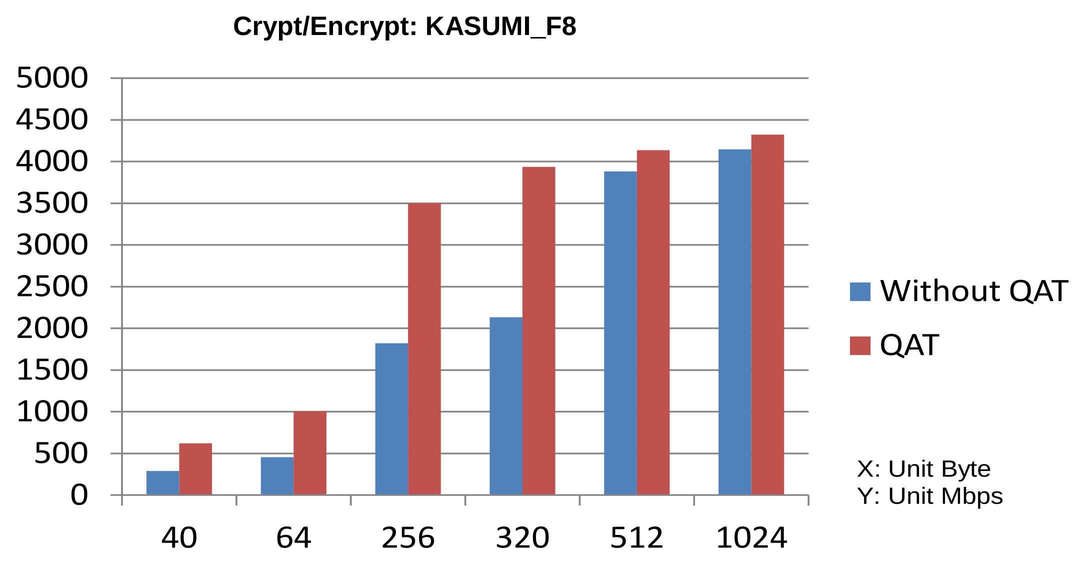


Figure 4

The packet flow within QuickAssist actually benefits from. Small encrypt packet performance sees the difference.

PKE Performance:

Operation	Curve	Req/sec
ECDSA Verify	P-384	1004

Key Size\ RSA with CRT	Req/sec
1024	12319
2048	2411
4096	327

As for DIFFIE-HELLMAN PHASE 2, result shows modulus size 2048 (bits) with 7082 (ops/sec), and 4096 (bits) with 1414 (ops/sec). CPU B915C pairs with 2 core and 4 threads. The test utilizes 2 threads only. However, performance is tremendously especially at small packet size. Also, packet with crypt in network performance is increased substantially.

The Test 2:

Build IPsec tunnel by QuickAssist and compare packet performance.

This software generates a GNU*/Linux* kernel module that accelerates some of the cryptographic algorithms in the Linux* Kernel Cryptographic Framework (LKCF) using the Intel® QuickAssist Technology implemented on Crystal Forest based platforms.

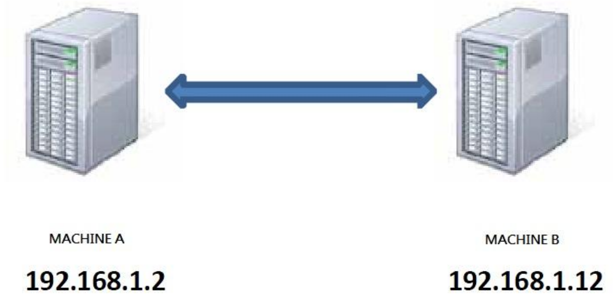
Specifically, it registers an implementation of the asynchronous Authenticated Encryption with Additional Data (AEAD). This software also adds a standalone test module and uses strongSwan* IPsec software to test the sample kernel module driver.

- **Use Algorithm:** AES128 CBC with HMAC-SHA-1
- **Supported:** Supported IPsec mode is Encapsulating Security Payload (ESP). Authentication Header (AH) mode is NOT supported
- **Supported:** IPsec protocol is IPv4 protocol. IPSec for IPv6 is NOT supported
- **Supported:** Supports both Tunnel and Transport mode of IPsec

IPsec limitation:

The Linux* Kernel Cryptographic Framework Sample Driver for Intel® QuickAssist Technology has the following limitations:

- Authentication Header (AH) mode is not supported
- IPsec for IPv6 protocol is not supported
- The sample driver is provided as a proof of concept only

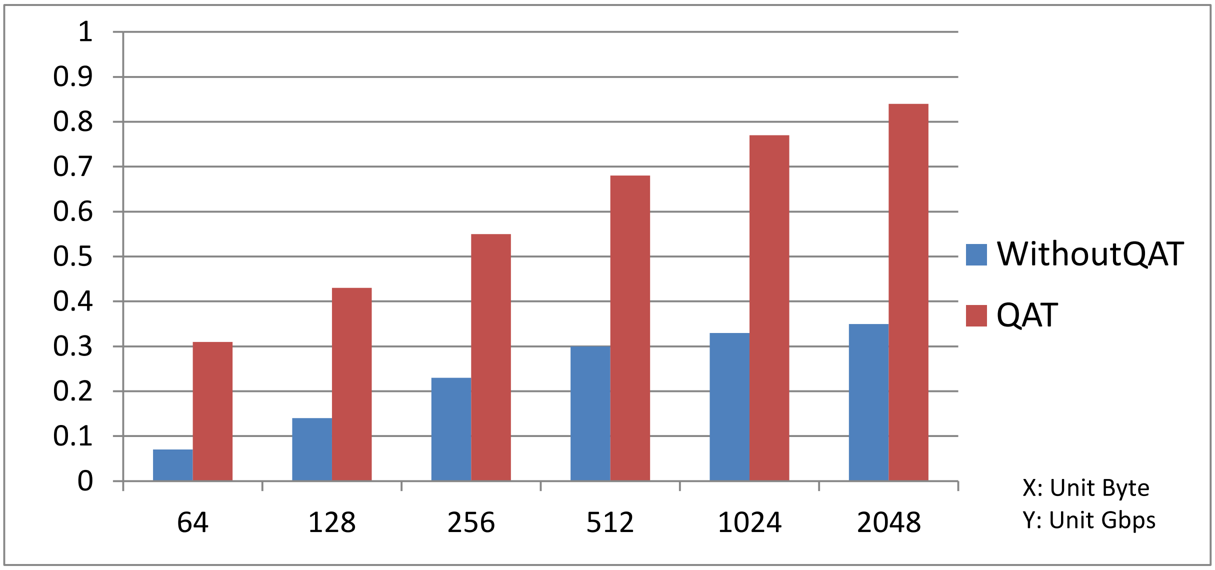


Hardware:

Connected two NA-360 hardware platforms, Stargo/Gladden 4C 1.5GHz, Quick Assist DH89003 B0 version.

Software Requirement:

- Operating system: Fedora* 16 64-bit version
- Kernel: GNU*/Linux* 3.1
- Crystal Forest Software for Linux* version 0.9.0
- Ipsec Software package strongSwan*: strongSwan* version 4.5.3
- Netperf Software: Netperf version 2.6.0



Quick Assist Device accelerates IPsec tunnel transaction in 64 byte,128 byte, 256 byte, 512 byte. Result demonstrates QAT benefits network application which applied on recent Intel® Crystal Forest platform. The QAT Technology Accelerator Abstraction Layer allows a software framework for deploying platform-level services and abstracting the interconnect technology from the application code providing resource management and provisioning services. That enables more efficient use of costly accelerator resources by allowing them to be transparently shared amongst multiple workload clients.

For more information of NA-360, please browse Axiomtek global website www.axiomtek.com. Or you may e-mail to info@axiomtek.com.tw to require more data.