

An Efficient Design of High Speed Network Security Platform using Network Processor

Yong-Sung Jeon, Sang-Woo Lee, and Ki-Young Kim
Electronics and Telecommunications Research Institute
161 Gajeong-Dong, Yuseong, Daejeon, 305-350, KOREA
Tel.: +82-42-860-5855, Fax.: +82-42-860-5611
E-mail: ysjeon@etri.re.kr

Abstract: *The explosive growth of internet traffic and the increasing complexity of the functions performed by network nodes have given rise to a new breed of programmable micro-processors called network processors. Network processors are emerging a programmable alternative to the traditional ASIC-based solutions in scaling up the data plane processing of network services. This paper proposes a design method and a hardware architecture of high speed network security platform using the IXP2850 network processor. It describes why the Intel IXP2850 network security equipment is an attractive platform for developing the protocol.*

Keywords - Network processor, Network security, IXP2850

1. Introduction

The Intel IXP2850 network processor is a member of Intel's second-generation network processor family. Based on the first-generation Intel IXP1200, the IXP2850 is a programmable network processor that integrates a high-performance parallel processing design on a single chip for processing complex algorithms, deep packet inspection, traffic management, and forwarding at wire speed. Its store-and-forward architecture combines a high-performance Intel xscale core with sixteen 32-bit independent multi-threaded microengines that cumulatively provide more than 22.4 giga-operations per second[1][2].

The microengines provide the processing power to perform tasks that traditionally required expensive high-speed ASICs. The Intel IXP2850 Network Processor is a powerful packet forwarding and traffic management processor for up to 10Gbps network edge and core applications. The IXP2850 Network Processor features a built-in SPI-4.2 interface for both framers and switch fabrics.

By performing stackless operations against packets, network processors improve performance and offer increased flexibility for selecting packets for inspection, thus dramatically reducing system bandwidth use while addressing high data rate problems. Although flexible in their treatment of header fields, they aren't fast enough to maintain performance on complex network security processing tasks. Fortunately, with significant advances in configurable logic such as FPGAs and associated custom memories like ternary content-addressable

memories(TCAMs), system designs can provide flexibility while maintaining high performance.

Network processors and FPGAs provide powerful, high data rate programmable and configurable logic. Ternary content-addressable memories, also called network search engines, provide high-speed table lookups for switching access-control lists(ACLs) to user name lists. Classification coprocessors using FPGAs provide bulk payload or field-level analysis and comparison of patterns or keywords to use in conjunction with correlative algorithms to determine traffic intent[3].

2. Intel IXP2850 Architecture

Figure 1 is a simple block diagram of the IXP2850 network processor showing the major internal hardware blocks[4]. The IXP2850 family is one of Intel's recent network processor product lines based on their Internet Exchange Architecture. It has sixteen RISC processors, called microengines, plus a XScale processor. The microengines are geared for data plane processing and have hardware support for eight threads that share a program memory. The microengines have access to all shared resources(SRAM, DRAM, MSF, etc) as well as private connections between adjacent microengines.

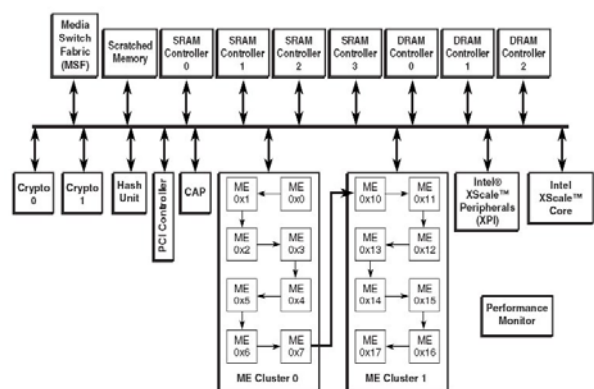


Figure 1. Functional Block Diagram of the IXP2850 Network Processor

The IXP2850 has the PCI controller that provides a 64-bit, 66MHz capable PCI Local Bus Revision 2.2 interface. It is also compatible to 32-bit and/or 33MHz PCI devices. The PCI controller provides the many functions like target access(external bus master access to SRAM, DRAM, and CSRs), master access(the Intel

XScale core access to PCI target devices), two DMA channels, and PCI arbiter.

The XScale core of IXP2850 governs the initialization of the whole system and part of the packet processing. The XScale core typically manages the control plane of the network processor where it processes exception packets, chip configuration and control, as well as managing route table entries and running signaling stacks. The IXP 2850 has a slow port that is an external interface, used for flash ROM access and 8,16, or 32-bit asynchronous device access. It allows the Intel XScale core do read/write data transfers to these slave devices.

The memory architecture for the IXP2850 is divided into several regions : large off-chip DRAM, faster external SRAM, internal scratchpad. DRAM is the initial storage area for packets while they are being processed. DRAM also stores large data structures such as route tables and flow descriptors. The SRAM interface is used for tables, buffer descriptors, free buffer lists and for interfacing coprocessors such as Ternary Content Addressable Memories(TCAMs) and classification coprocessors. Typically SRAM is storage area for variables and packet state information. The scratch memory is often used for internal microengine-to-microengine communication and local data storage.

The Media and Switch Fabric(MSF) interface is the primary interface for transferring network packets. The MSF connects to MACs and framers with industry standard interfaces such as SPI4-2. Because the MSF is in between the MACs and framers and the microengines, which handle the bulk of the packet processing, the MSF needs to buffer the packets effectively as they enter and leave the chip.[5] And, MSF consists of separate interfaces for receiving and transmission. Each of interfaces can be separately configured for either SPI-4.2 for PHY devices.

The special feature of the IXP2850 is having a crypto core which integrates two crypto units for performing bulk crypto operations. The IXP2850 has exactly the same architecture of the IXP2850 with the addition of the internal crypto functionality. The purpose of the IXP2850 is to do bulk encryption and decryption at 10 gigabits per second, providing supporting protocols for robust applications such as VPN/firewalls, SAN/NAS storage gateways, secure web servers, L5-L7 traffic management systems, and the like. Adding crypto to the internal architecture has significant performance and cost benefits.[5]

3. Design of Network Security Platform using the IXP2850

Figure 2 shows the hardware architecture of network security system that we propose. This stand-alone type system uses the IXP2850 network processor. This system is divided into two parts. One is NPU card that contains the IXP2850 network processor and the memory device like RDRAM, QDRSRAM, TCAM,

flash ROM. Especially this NPU card has a Boot ROM to recover the OS code contained in a flash ROM. The other is Ethernet line card that contains Media Access Controller (MAC) chip, Ethernet Physical layer (PHY) chips, media ports, and management ports like serial port and Ethernet port. These cards are joined with two connectors. One is for the SPI-4.2 signal connection. The other is for the PCI signal, management ports signal and power signal connection.

The detail description of architecture and function for the NPU card is as follow. The IXP2850 initializes the MAC chip and the Ethernet controller using the PCI interface that has 64-bit wide data path and 66-megahertz data transfer rate. The IXP2850 has four independent SRAM controllers, which each support pipelined QDR synchronous static RAM and/or a coprocessor that adheres to QDR signaling.

The each of three QDR SRAM channels in this paper has two QDR SRAM of 4Mbyte capacity. And, one of QDR SRAM channels has a TCAM and a FPGA. If the network processor retrieves the header fields, then it sends key header fields to the TCAM to check for matching packets. And, the FPGA is used for a classification coprocessor which searches a payload for particular patterns or signatures.

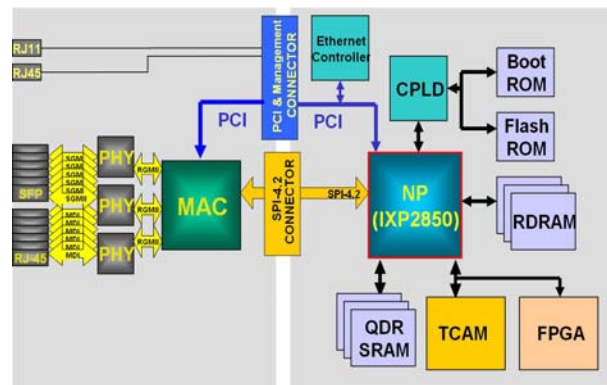


Figure 2. Hardware architecture of proposed network security platform

And, The IXP2850 has controllers for three Rambus DRAM(RDRAM) channels. Either one, two, or three channels can be enabled. When more than one channel is enabled, the channels are interleaved on 128byte boundaries to provide balanced access to all populated channels. Each channel for RDRAM in this paper has 256M bytes NexMod RDRAM module. Therefore, total capacity of RDRAM is 768M bytes.

The CPLD generates control signal for the boot ROM and the Flash ROM using the slow port signal of IXP2850. The boot ROM in this paper contains the recovery loader that has the functions to reload the codes of Flash memory. The socket-type Atmel EEPROM is used for the boot ROM. Therefore, In case the boot ROM code is damaged by unpredictable factor, the boot ROM could be changed easily. The Flash

memory contains codes for redboot, diagnostics, operating system and permanent data.

The NPU card also has the Ethernet controller for management port located in the Ethernet line card. This Ethernet controller is initialized and controlled by the IXP2850 through the PCI interface.

The detail description of architecture and function for the Ethernet line card is as follow. The MAC chip of the Ethernet line card is a twelve-port MAC device targeted for 10/100/1000 Ethernet aggregation applications. This MAC device supports multiple industry-standard RGMII interface that connect to off-the-shelf Ethernet physical layer devices. The PHY chips in this paper contain four independent Gigabit Ethernet transceivers on a single IC. The Ethernet line card uses three PHY chips and has the twelve media ports.

Additionally, the Ethernet line card has two management ports. One is serial port. The other is 10/100 Ethernet port. This management port transmits and receives the signal for monitoring and controlling the status of IXP2850. Finally, The power of the Ethernet line card is supplied form the NPU card by the additional pins of PCI & management connector.

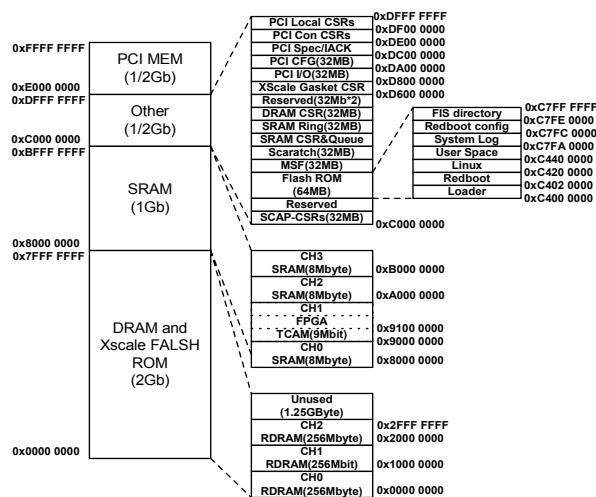


Figure 3. Memory map

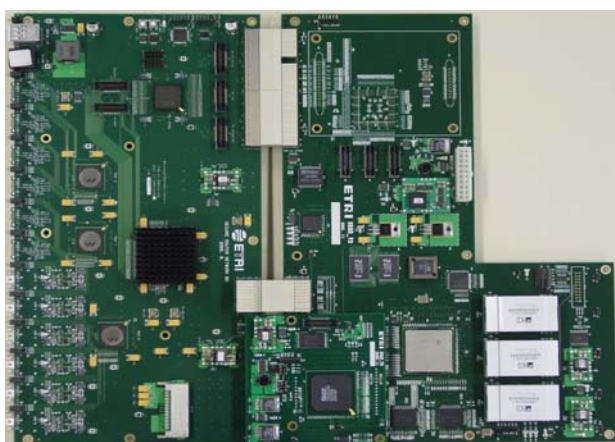


Figure 4. The network security platform

Figure 3 shows the memory map of proposed network security platform. Previous speaking, boot software is separated in two parts. A recovery loader is located in EEPROM and a normal boot loader is on the flash memory. The functions of the recovery loader are serial communication and burning a boot loader image on the flash memory. The boot loader used in this platform is the standard embedded system debugging and bootstrap environment from Red Hat. The boot loader contain functions of POST(Power On self Test), serial communication, Ethernet communication and flash management. Especially, the boot loader has BOOTP client to get IP network configuration and TFTP client to download code from the development server. Figure 4 shows the prototype of the network security hard ware platform proposed in this paper.

4. Conclusion

In this paper, we presented an efficient design method for a stand-alone type network security hardware platform using IXP2850 network process. For the flexibility of hardware architecture, the platform proposed in this paper is separated into two cards-the NPU card and the Ethernet line card. These cards are joined with connectors on the basis of standard interface signals like SPI-4.2 and PCI. Therefore, if you want to modify the number of media ports, you can change only the Ethernet line card. Similarly, if you want to modify the capacity or combination of memory for the IXP2850, you can change only the NPU card. Therefore, design method proposed in this paper is very helpful to upgrade the system. And, this paper proposed a good configuration of network security platform to check for matching header fields of packets and to search particular patterns or signatures of payloads of packets using the TCAM and the FPGA.

References

- [1] Madhu Sudanan Seshadri, John Bent, and Tevfik Kosar, "Intelligent Routing using Network Processors: Guiding Design through Analysis", October 2002.
- [2] Ying-Dar Lin, Yi-Neng Lin, Shun-Chin Yang, and Yu-Sheng Lin, "DiffServ over Network Processors: Implementation and Evaluation", *IEEE Proceedings of the 10TH Symposium on High Performance Interconnects Hot Interconnects Hot Interconnects*, 2002.
- [3] Peder Jungck, Simon S.Y., "Issues in High-Speed Internet Security", *IEEE Computer Society*, vol. 37, no. 6, pp. 36-42, July, 2004.
- [4] Intel Corp., "Intel IXP2800 Network Processor: Hardware Reference Manual", November 2002.
- [5] Bill Carlson, *Intel Internet Exchange Architecture and Applications*, Intel Press, 2004.
- [6] Niraj Shah, William Plishker, and Kurt Keyuzer, "NP-Click: Aprogramming model for the Intel IXP1200", *International Symposium on High Performance Computer Architectures*, February 2003.