

Bidirectional 1 Gbps Full-Wire Speed IPsec Processing Engine

FUJITSU is now mass-producing “MB86978” LSIs that can process the IPsec protocol at a full-wire speed of 100 Mbps in both directions. This advanced LSI is designed to enhance the throughput of the existing device tenfold to 1 Gbps in both directions.

Introduction

FUJITSU is developing an LSI that can process the IPsec protocol at a bidirectional full-wire speed of 1 Gbps. This new device is specifically designed for IPsec processing and thus it is expected to dramatically improve IPsec throughput and reduce the burden on CPUs for processing compared to the currently prevailing Lookaside^{*1}-type LSIs for encryption.

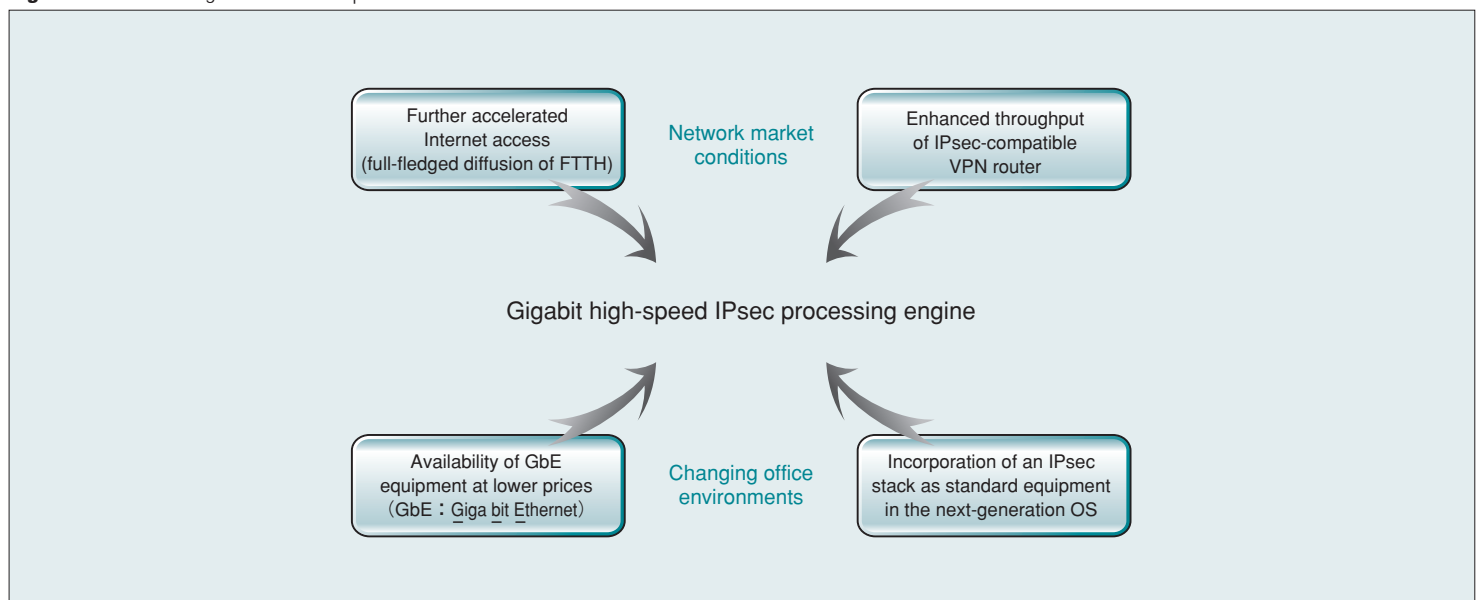
This device aims at being ideal LSI for advanced broadband environments of Internet connection and LAN. Coming advanced

environments require security, high-speed, low-delay, and low-fluctuation features.

Description of IPsec

IPsec is a technology that provides security for individual IP packets. It encrypts individual IP packets and then guarantees that the transmitted data is free from any falsification, thus enabling proper access control. Conventionally, security options

Figure 1 Market Background for Development



are provided for individual applications. However, the adoption of IPsec helps ensure higher speed and more secure transmission channels.

A current hot topic relating to Internet access involves the VPN that links key company offices via virtual dedicated lines to guarantee communications safety. IPsec is one of the protocols used to implement the VPN. It is also an optional protocol for IPv4 communication and it has been adopted as an essential protocol for the next-generation protocol IPv6 communication. As such, IPsec is expected to be widely utilized as a key technology in networking in the future.

Market Background and Development Concept

FUJITSU is developing this new device to keep up with the changing network market conditions and office environments.

With the spread of broadband networking and enhanced throughputs of IPsec-compatible VPN routers adopted in SOHO environments, the center side equipment is required to provide IPsec processing capability at gigabit-level speed. In office environments, as PCs are now coming out with Gigabit Ethernet ports and NICs and HUBs supporting the Gigabit Ethernet are available at lower prices, LAN is expected to allow gigabit speed in the near future.

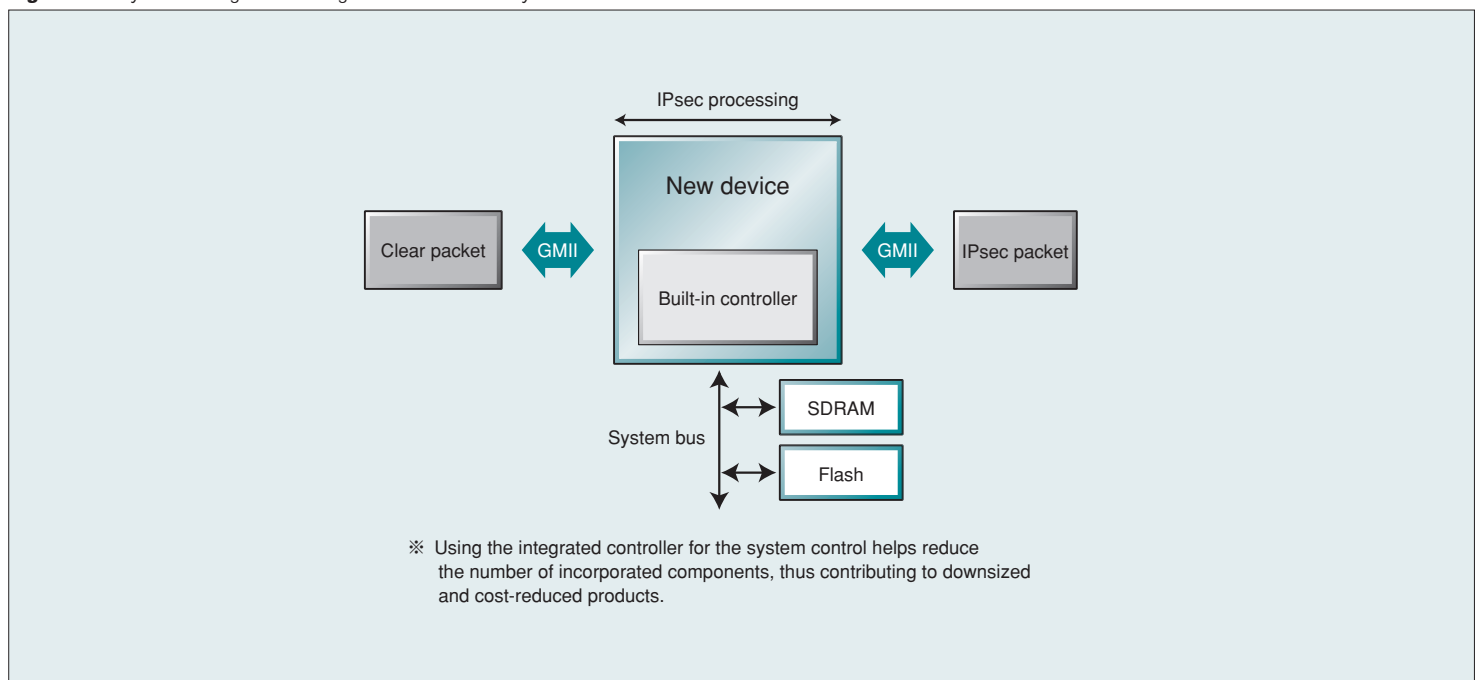
In addition, an IPsec stack is to be incorporated as standard equipment in Microsoft's next-generation OS scheduled to be released in the second half of 2006; this may start an era of full-fledged IPv6 communication. With an increased number of PCs running this next-generation OS, the utilization of IPv6 packets in LAN will increase and, as a result, printers and MFPs (multi-functional peripherals) connected to the LAN will be required to offer IPv6 compatibility. These peripherals differ from PCs in CPU performance and therefore, for ultra-high-speed IPsec processing, the installation of an IPsec accelerator (engine) is indispensable.

To keep up with the above-mentioned trend, FUJITSU considers the development of a gigabit-level high-speed IPsec processing engine to be of the highest priority.

Fig.1 presents the market background for the development of the new device.

FUJITSU has already succeeded in developing LSIs that implement bidirectional 100 Mbps full-wire speed transmission and encryption. At the time, the Lookaside architecture encryption engine was prevailing in the market, and it was known that CPU performance enhancement would be the only solution for improved IPsec processing throughput. As such, FUJITSU adopted in-line architecture for LSIs to reduce the burden on CPUs and implemented a bidirectional 100 Mbps full-wire speed. The new device also adopts similar in-line architecture and incorporates a special controller that supports

Figure 2 A System Configuration Using New Device (Security BOX)



the processing of IKE*2 and other protocols to cover the entire IPsec processing on a single chip. The new device also contains an IKE engine interface (PCI bus), allowing it to rely on the main CPU for processing of the IKE protocol without using the special controller.

Fig.2 presents one system configuration (Security BOX) using this new device.

Fig.3 illustrates another system configuration (Middle-Range VPN Router) using this new device.

The new device enables the processing of IPsec at a full-wire speed, despite the packet size. This device is aimed to become an essential LSI solution for communication via the VPN in the coming high-speed broadband age and also for IPv6 communication through ultra-high-speed LAN systems.

Product Features

Equipped with GMII/RMII/MII*3 interfaces

- One port on each side: WAN and LAN (a total of two ports)
- GMII/RMII/MII modes can be set
- Equipped with an SMI interface for PHY device control

Configured with an IKE-specific controller and an IKE engine

A specialized controller for the full support of IKE is

incorporated. In addition, an engine supporting arithmetic operations is incorporated for the accelerated computation of IKE. The interface is a 32-bit PCI bus.

Configured with an IPsec processing engine

To implement the IPsec protocol at a full-wire speed, the following capabilities are incorporated.

- Full-wire encryption engine: DES/3DES*4 (CBC mode)
AES*5 (CBC mode, key length 128/192/256 bits)
- Full-wire authentication engine: HMAC-SHA-1*6
HMAC-MD5*6
AES-XCBC*7
- SA*8 database: Available setting of up to 512 SAs (Encoding direction: 512, Decoding direction: 512)

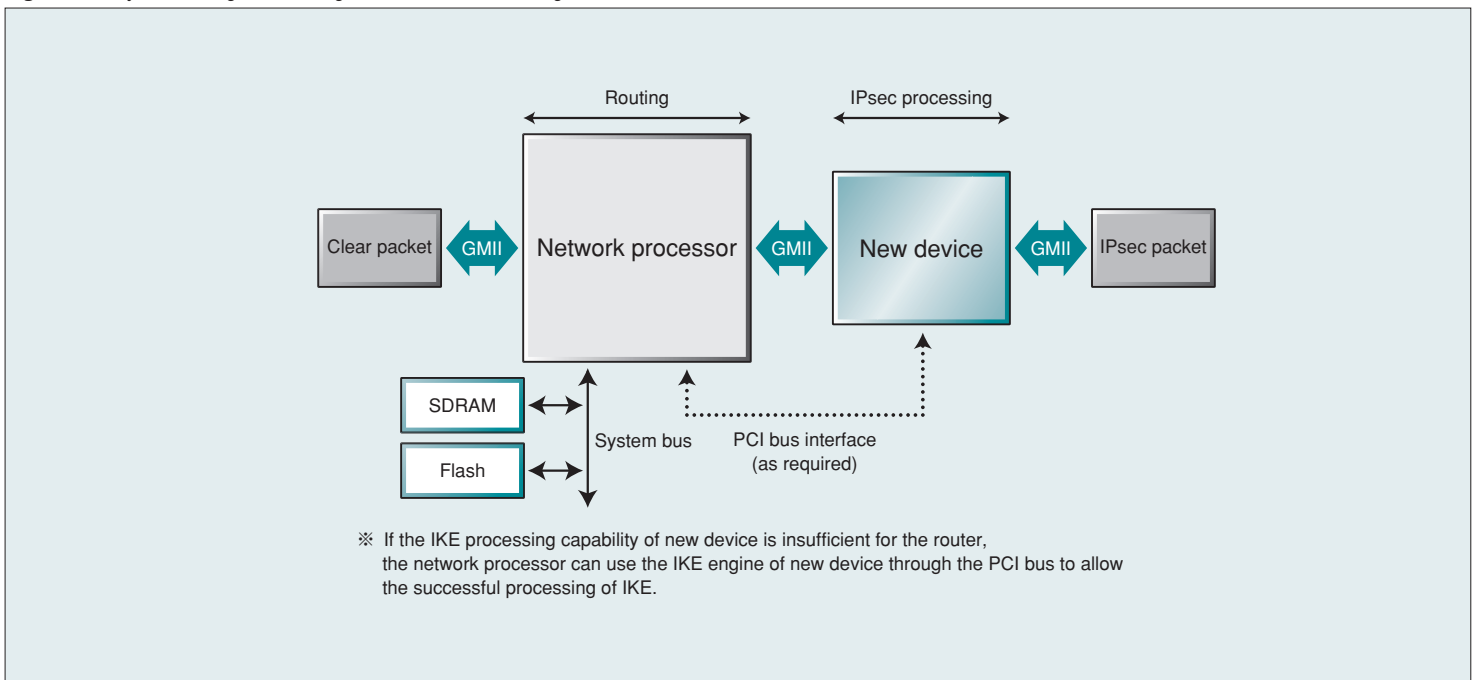
Applicable packet

- PPPoE packet
- VLAN*9 packet
- Compatible with both IPv4 and IPv6
- Compatible with NAT-Traversal*10

Available mode

- Transport mode (ESP*11, AH*12, ESP, and AH)
- Tunnel mode (ESP, AH)
- Transport over tunnel mode

Figure 3 A System Configuration Using New Device (Middle-Range VPN Router)



■ Auto-fragment, reassembly functions

Any packets that have a packet length exceeding the MTU size after IPsec processing may be automatically divided into two fragments. The fragments of an IPsec packet may be reassembled into the original packet.

■ Compatible with Jumbo Frame^{*13} (up to 9 Kbytes)

Development Environment

FUJITSU is also developing an evaluation platform to support customers in speedy product development. ITRON and Linux will be adopted as the OS. *

NOTES

- * 1: Lookaside: A methodology used to connect to the CPU via the system bus.
- * 2: IKE (Internet Key Exchange): A protocol to authenticate the destination of the communication and exchange the secret key used for IPsec.
- * 3: GMII/RMII/MII: A standard for interfacing with PHY (physical layer).
- * 4: DES (Data Encryption Standard): A secret-key encryption algorithm. 3DES involves the triple application of DES.
- * 5: AES: An advanced secret-key encryption algorithm that may replace the DES.
- * 6: HMAC-SHA-1, HMAC-MD5: An authentication system to check for any falsification of communication data.
- * 7: AES-XCBC: A method using AES as the message authentication code (MAC)
- * 8: SA (Security Association): A logical transmission channel in which the sender, receiver, security protocol, and other transmission parameters are properly defined.
- * 9: VLAN (Virtual LAN): A technology to develop a virtual terminal group in a LAN, regardless of the type of physical connection.
- *10: NAT-Traversal: A technology to implement IPsec through NAT.
- *11: ESP (Encapsulating Security Payload): A security protocol used for encryption.
- *12: AH (Authentication Header): A security protocol used for authentication.
- *13: Jumbo Frame: A technology used to increase packet size for enhanced data transmission efficiency in the Gigabit Ethernet
- * Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.
- * Linux is either a registered trademark or trademark of Linus Torvalds in the United States and/or other countries.