Using the IP Security Hardware Assist Feature of the IBM 10/100 Mbps Ethernet PCI Adapter II (F/C 4962)

Document Number: WP100297
www.ibm.com/support/techdocs
Last revised: 15Aug02

Introduction

The 10/100 Mbps Ethernet PCI Adapter II (F/C 4962) is a small form factor, single port PCI Ethernet adapter. This high performance, low power Ethernet 10/100Mbps LAN adapter can be used in both client and server PCI systems. The 10/100 Mbps Ethernet PCI Adapter II provides both 10Base-T and 100Base-TX full duplex Ethernet LAN connectivity. The adapter supports Category-5 unshielded twisted pair cabling for both 10/100 Mbps and Category-3 unshielded twisted pair cabling for 10 Mbps.

After 4/26/02, the 10/100 Mbps Ethernet PCI Adapter II supports the offload of IP Security (IPSec) cryptographic algorithms by providing hardware assistance in performing data encryption and authentication.

The cryptographic algorithms to be offloaded to the adapter are:

- Data Encryption Standard (DES)
- Triple DES

The authentication algorithms to be offloaded to the adapter include:

- HMAC
- MDA5
- HMAC SHA.

IPSec packet encryption and authentication is achieved with the use of Authentication Header (AH), Encapsulated Security Payload (ESP) or a combination of AH and ESP. Without the offload feature these IPSec encryption functions are done in the host, causing degradation of throughput and higher CPU utilization. Offloading these functions to the hardware will generally provide higher throughput with lower CPU utilization.

IPSec is the building block for Virtual Private Network (VPN) support. VPNs support secure, private connections among corporate users (the Intranet), business partners (the Extranet), off-site employees/tele-commuters (Remote Access) and customers (e-commerce), all using the Internet as the transport facility.

Software Requirements

This IPSec hardware assist support is provided with AIX 5.1 (with appropriate software updates) and later software. This function, normally performed with encryption software by the host, is offloaded to the adapter, which performs the outbound encryption and inbound decryption on behalf of the host software. To invoke the IP Security function on the adapter, you must obtain AIX 5.1 software updates IY27069 and IY26514 or the 5100-02 Recommended Maintenance package. These updates can be obtained by ordering APAR IY28102, or by ordering theAIX 5.1 Update CD (LCD4-1103-03) dated 4/2002 or later.

Note: This IP Security function is not supported with AIX 4.3 software.

Enabling IPSec Hardware Assist

The IPSec hardware assist function is disabled by default and must be explicitly enabled. Enablement of the IPSec offload function for the IBM 10/100 Mbps Ethernet PCI Adapter II is supported by all of the AIX system management interfaces (command line, smit, smitty, WebSM). From the user prompt the following commands can be used:

```
    lsattr -El entx                       (to view the ipsec_offload attribute)
    chdev -l entx -a  ipsec_offload=yes   (to enable IPSec offload operation)
    chdev -l entx -a  ipsec_offload=no    (to disable IPSec offload operation)
```

The ‘smit chdev’ fast path may also be used to control this function. The *IPSec Offload* option has been added to the IBM 10/100 Mbps Ethernet PCI Adapter II smit menus and dialogues. This option takes a “yes” or “no” value.

The IP interface device associated with this adapter must be brought down using the following command sequence before the ipsec_offload option can be modified:

```
                ifconfig enx inet down
                ifconfig enx detach
```

IPSec Statistics

All of the IPSec related information will be logged and maintained by the device driver as part of the statistics of the network device driver. Enhancements have been made to the AIX *entstat* command to allow the display of this information and to verify that the offload function is actually working. For example, to display the Ethernet device generic statistics and the Ethernet device-specific statistics with IPSec-related information for ent0, enter:

```
   entstat -d ent0
```

Information provided by this command includes:

- Transmit IPSec packets
- Transmit IPSec packets dropped
- Receive IPSec packets
- Receive IPSec packets dropped
- Inbound IPSec SA offload count

The *netstat -v* command will also provide these statistics.

Hardware Limitations

- F/C 4962 does not support IPSec offload of fragmented packets. The AIX IPSec driver checks the size of the packet that would be sent out by the adapter and if it is greater than the MTU size, such packets will be processed by the AIX IPSec driver and not offloaded.
- F/C 4962 does not handle keyed authentication. It only supports HMAC-MD5 or HMAC-SHA1 authentication through ESP or HA but not both.
- F/C 4962 only supports the IPSec offload of the IPv4 packets. It does not support the IPSec offload of IPv6 packets and packets with IP options.

IPSec Offload Performance

Lab measurements have verified significant increases in throughput and reduced CPU utilization through the use of the IPSec offload function. IPSec operations are computational intensive, therefore relative performance improvements will vary depending upon the processor model in question and the authentication/encryption algorithms used. In general on systems with slower CPU speeds, the raw throughput performance improvement will be the most significant. On faster machines the relative improvement may be less as the processors are more able to keep the adapter busy. And for any given throughput, the CPU utilization will be reduced since the bulk of the IPSec workload is being transferred to the adapter hardware.

The following table illustrates the improvements that were measured when comparing IPSec with and without offload enabled:

Encryption Algorithm	Authentication Algorithm	Streaming Direction	Raw Throughput Improvement	Peak CPU Utilization
3DES	HMAC/MD5	Simplex	449%	-37%
	HMAC/MD5	Duplex	587%	+10%
	HMAC/SHA	Simplex	460%	-31%
	HMAC/SHA	Duplex	671%	+18%
	Keyed/MD5	Offload not supported by adapter		
DES	HMAC/MD5	Simplex	249%	-19%
	HMAC/MD5	Duplex	290%	+7%
	HMAC/SHA	Simplex	270%	-20%
	HMAC/SHA	Duplex	334%	-12%
	Keyed/MD5	Offload not supported by adapter		

Note: These measurement were made using a 340MHz RS64-II based processor.

References

AIX 5L Version 5.1 System Management Guide: Communications and Networks, “Internet Protocol (IP) Security”.