

網路 IC 產品線分析

謝才俊、林盈達

國立交通大學資訊科學研究所

新竹市大學路 1001 號

前言

網際網路的蓬勃使用帶動了整體網路產業的進步，新的網路通訊設備也不斷的被開發出來。在網路設備當中不但需要有軟體程式來付予它各式各樣的功能，更重要的是要有硬體元件來執行程式所下達的命令，甚至於加速程式的運行。

這篇文章將介紹網路設備中所使用到的 IC 元件，包括有網路卡(NIC)控制晶片、交換式集線器(Switch HUB)控制晶片、網際網路處理器(Internet Processor)晶片、網路安全(Network Security)晶片以及網路處理器(Network Processor) 等晶片。並且將簡要的說明及分析 IC 規格表當中所提出的功能，最後將探討網路 IC 未來的趨勢。

1. 網路 IC 的分類

網路的產品遍佈於我們的生活當中，在此我們以 Internet TCP/IP 的五層 Layer 來做為劃分的標準，在五層 Layer 當中，愈低層代表愈接近傳輸媒介(Media)，愈高層代表愈接近使用者介面(User Interface)。我們以圖一來表示出不同的網路晶片所處的地位。

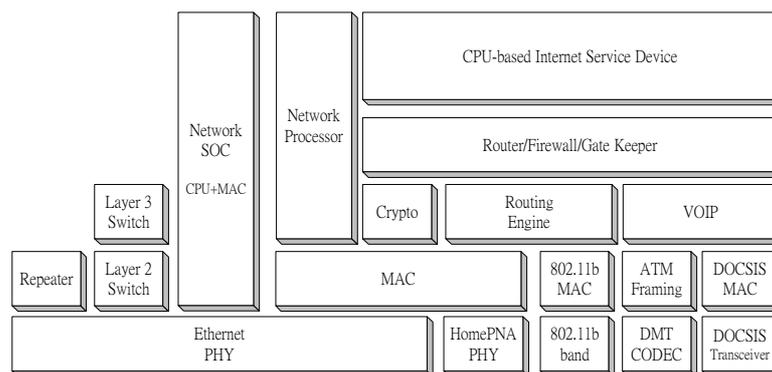


圖 (一) 網路晶片分佈

我們可以先將現有網路產品歸為三類，再分別對每一類產品中所使用到的晶片來一一做說明：

- (1) Layer1，Layer2 的網路產品我們稱之為網路存取設備(Access Device)
- (2) Layer3，Layer4 的網路產品我們稱之為網路核心設備(Core Device)
- (3) Layer5 以上的網路產品我們稱之為網路服務設備(Service Device)

在 Layer 1 的網路晶片，因為所要處理的是類比傳輸訊號到數位信號之間的轉換，如果是用數位信號處理器(DSP)來實現，就可以比用 ASIC 製作達到最多的彈性。

在 Layer 2 到 Layer 4 的網路晶片因為所要處理的資料是網路上的通訊協定。這些通訊協定所要傳遞的封包格式有工業上的標準來規範。所以很合適以專門的 ASIC 來實現。

Layer 5 以上的網路設備因為它們所要執行的功能常常需要隨著網際網路(Internet)的發展而有所變更，所以傳統上這類設備都是以 General Purpose CPU 配合軟體來完成。但是近年來因為網路傳輸速率的不斷提昇，這種架構已漸漸無法負荷網路頻寬的需求，所以目前已經有許多專門的 ASIC 出現，用於各層所需的加速處理(即減輕的負荷)，例如路由查詢 ASIC、加/解密加速器 ASIC 及網路處理器(Network Processor)晶片等，它們都是希望利用硬體電路來處理網路上的封包，解決網路頻寬的瓶頸。另外也有將 CPU 與原本獨立的其它 ASIC 整合成一顆單晶片，即 SoC(System On Chip)，除了可以讓速度變快，更可大幅降低系統成本。以下我們將分析比較這三類網路設備中所使用的晶片。

2. 網路存取設備當中所使用的 ASIC 元件

首先先介紹在網路存取設備中所使用到的晶片，這一類網路設備主要的功能是負責去處理網路傳輸時的電氣信號和通訊協定(Protocol)，如果以網路架設的範圍來看，也可以說是屬於區域網路(Local Area Network, LAN)的範圍，目前在區域網路當中最主流的通訊協定是 IEEE 802.3 Ethernet 系列。本文將著重於此系列所衍生出的產品的介紹。

在區域網路當中為了要讓每台電腦之間能夠互相通訊，有兩種網路設備是必須的。一是網路卡 (NIC)，二是集線器(HUB)。我們首先來介紹網路卡所使用的控制晶片：

2.1 Ethernet 網路卡控制晶片

一張 Ethernet 網路卡的控制晶片是由三部份電路所組成，分別是 MAC 晶片，實體層(PHY)晶片，及收發器(Transceiver) 晶片。

MAC (Media Access Controller)

MAC 晶片的組成單元可細分為三部份子電路，分別是通訊協定控制器(Protocol Controller)，緩衝記憶體管理(Buffer Memory Management) 電路，以及匯流排界面電路(BUS Interface)。底下就針對這三部份電路做一說明：

第一部份- Protocol Controller

Protocol Controller 電路是用來處理 IEEE 802.3 CSMA/CD 的演算法，包含封包的收

送，偵測碰撞(Collision)現象，重送機制(Backoff)等。它對外和 PHY 溝通的界面在 10M/100M 網路卡控制晶片是採用資料寬度為 4 Bits 的 MII (Media Independent Interface)界面，到了 1000M 網路卡控制晶片則是採用資料寬度為 8 Bits 的 GMII(Gigabit Independent Interface)界面。

第二部份- Buffer Memory Management

Buffer Memory Management 電路，Protocol Controller 會將收到的資料先暫存到內部 FIFO Memory 當中，等到晶片取得系統匯流排的控制權後，Buffer Management 負責將 FIFO 中的資料搬移至系統記憶體當中，如果以資料存取控制的方式來區分，又可分為傳統以 I/O Mode 存取資料的 NE2000 相容模式，以及目前較為流行利用 Descriptor List 配合 BUS Master 來搬移資料等兩種方式。前者資料搬移的速度將受限於 CPU 執行 I/O 存取命令的頻率，後者因為網路卡晶片可以直接控制系統記憶體的匯流排，所以資料搬移的速度會比較快及有效率。

第三部份- BUS Interface

BUS Interface 電路，主要是負責 NIC 和 Host CPU 之間資料的傳遞，在個人電腦上使用的 10M/100M 網路卡大多是採用 32 Bits PCI Bus，只有伺服器上使用的網路卡或 1000M 網路卡才會用到 64 Bits PCI Bus。在筆記型電腦上則是採用 PCMCIA Bus 或 CardBus 來做為傳遞資料的界面，在 Embedded System 上因為考慮到系統的簡化，傳遞資料的效率反而是其次。所以會使用到 ISA Bus 來當做界面。

實體層(PHY)晶片

在實體層晶片方面，因為它牽涉到信號的傳輸媒介，為了讓不同廠商生產的網路設備都能夠互相連接起來，IEEE 和其它相關制定標準的單位制定了許多國際標準來規範通訊的方式，例如：10M/100M Ethernet 的 IEEE 802.3u，1000M Ethernet 的 IEEE 802.3ab，無線網路的標準 IEEE 802.11b，家用電話線網路的標準 HomePNA 1.0，HomePNA 2.0，ADSL MODEM 的標準 ITU G992.2(G.Lite)，ITU(International Telecommunications Union)，Cable MODEM 的標準 ITU J.112(DOCSIS)，DOCSIS(Data Over Cable Service Interface Specification)等等。這些標準的內容不外乎是規定傳輸速率，調變方式(modulation)，信號品質，通訊協定(Protocol)等等。

以 10M/100M Ethernet 使用的 IEEE 802.3u 標準為例，就規範了實體層(PHY)晶片的主要功能，包括 4B/5B Encode/Decode、scrambler/descrambler、auto-negotiation 等。先由 Auto-negotiation 負責和對方協商出兩邊網路卡都能夠執行的連線速度，然後將雙絞線收發器送過來的 5 個 bits 的資料去在除控制碼後，變成 4 個 bits 的數位資料，最後將此資料經由 MII 界面送給 MAC 來使用。

收發器(Transceiver)晶片

收發器晶片的主要功能是處理網路最前端的電氣信號，將網路線上串列資料的電氣

信號轉變為並列的數位信號，再將此數位信號傳遞給實體層(PHY)晶片來接收，這顆晶片的功能須要由類比電路的技術來達成，目前較為常用的設計方法是利用 CMOS 電路來完成。但是其良率會受到製程很大的影響。為了讓良率不受到製程的影響，所以也有的廠商是利用 DSP 技術來完成收發器的功能，但是相對的晶片的成本也將會提高

三合一晶片

所謂三合一晶片，就是將網路卡控制晶片中 MAC、PHY、Transceiver 這三部份電路作垂直整合，變成單一晶片。在國內，10M/100M Ethernet PCI 三合一網路卡控制晶片出貨量最大的是瑞半導體(Realtek)[1]出品的 RTL8139 系列，10/100M Ethernet PCMCIA 三合一網路卡控制晶片出貨量最大則是亞信電子(ASIX)[2]出品的 AX88790 系列。至於 10/100/1000M 網路卡控制晶片，目前國內廠商大都只推出純 MAC 的控制晶片，如大智電子[3]的 TC9021，三合一的 10/100/1000M 網路卡控制晶片目前只有幾家國外大廠有推出，如 BROADCOM[4]的 BCM5701。

新技術的支援

為了減輕 CPU 在處理網際網路封包時的負擔，Internet Protocol 的處理已經被加入至網路卡控制晶片當中，例如 National Semiconductor [5] 的 DP83820 晶片加入了 IP、TCP、UDP 的 Checksum 計算，並增加了對 802.1Q VLAN tagging 的支援，即當收到一個含有 VLAN tag 的封包時可以自動的將 VLAN tag 去除，也可將 VLAN tag 自動加到要送出的封包當中。同時也支援 802.1D、802.1Q priority queuing。

2.2 集線器(HUB)晶片

目前的主流集線器晶片是交換式集線器(Switch HUB)晶片。交換器所要處理的資料包含實體層和資料鏈結層二層。一般對於只處理到資料鏈結層資料的交換器我們稱之為第二層交換器(Layer 2 Switch)。如果是第三層交換器(Layer 3 Switch)就必須能夠處理到網路層(Network Layer)的資料，即利用 IP Header 來判斷封包的路由。一個完整的 Layer 2 交換器晶片是由以下數個電路所組合而成：

2.2.1 MAC 電路

它的功能同我們在介紹 NIC 時所介紹的 MAC 是一樣的，只是如果是 8 Ports Switch HUB Controller，它的內部就需要用到 8 個 MAC。

2.2.2 地址解析電路(Address Resolution)

決定封包路徑的電路我們稱之為地址解析電路(Address Resolution)，我們可以在 Switch HUB 的規格表上看到說某個 Switch HUB 可以記錄到多少個 MAC Address 指的就是這個部份電路處理 Lookup Table 的能力，一般來說 8 Ports Switch HUB 至少可以在 Lookup Table 當中記錄 1024 個 MAC Address 地址。地址解析電路又是由下面三個子電

路所組合而成:

地址學習電路(Address Learning)

它是將輸入封包的來源地址(Source Address)經由 Hash 演算法求得到一個指向內部 Lookup table 的地址，再將來源地址和來源埠兩項資訊一起記錄至 Lookup table 當中。

地址搜尋電路(Address Lookup)

它是將輸入封包的目的地地址(Destination Address) 經由 Hash 演算法求得到一個指向內部 Lookup table 的地址，利用此地址將已記錄在 Lookup Table 當中的資料拿出來和封包中的目的地地址做比對，如果發現有符合的地址就通知接收電路將此封包交由查詢到的埠來傳送，如果沒有發現有符合的地址，則就將此封包廣播給所有的埠。

計算記錄壽命電路(Aging)

它會重複地去檢查 Lookup Table 中的每一項記錄，並將檢查過的資料項中的 aging 欄減去一，如果此欄的值被減為零，則代表此項資料已經很久時間沒有電腦來使用到。為了讓 Lookup Table 可以服務更多的機器，計算記錄的壽命電路會自動地將此記錄由 Lookup Table 中永遠刪除，以防止過時的記錄繼續霸佔著 Lookup Table 記憶體的空間。最後導致 Lookup Table 無法記錄新的資料。

2.2.3 交換核心 (Switching Fabric)

Switch 從地址解析電路得到目的地的 Port 後，接下來必須將封包放入交換核心中送往輸出的 Port，目前有兩種架構常用來實現交換核心電路。

Crossbar

每一個輸入 Port 通過一個交叉點開關和輸出 Port 相連接，建立一個專屬通道，一個 N Ports 的交換核心就須要個 $N \times N$ 個交叉點開關，每一交叉點開關須要大量的連線，當 Port 數增加時，其硬體複雜度也將快速的增加。一般來說，只有在須要頻寬高達數十 G 的系統才會使用到這樣的架構。

Shared Memory

每一個輸入 Port 的封包都寫入到同一個 Shared Memory 當中，當每一個輸出 Port 的 Output Queue 中有需要輸出的封包到達時，Output Port 就到 Shared Memory 當中讀出封包送出，要滿足所有的 Port 同時進行一讀一寫的操作，還能夠達到 Wire Speed 的要求，其記憶體所需要的頻寬為 Port 數乘以線上傳輸速度(Wire Speed)的兩倍，以 8 Port 100Mbps Switch Hub 為例，其所需要 Shared Memory 的頻寬為 $8 \times 2 \times 100M = 1.6 G$ 。目前大部份中低價位的 Switch Hub 晶片採用的都是這樣的架構。

2.2.4 封包暫存記憶體管理電路

目前的 Layer 2 交換器大都支援封包儲存再轉送(Store and Forward)的機制，所以交換器需要使用大量暫存 Packet 的記憶體，目前有外接記憶體(External Memory)及嵌入記憶體(Embedded Memory)兩種作法：

外接記憶體(External Memory)

目前採用外接記憶體方式的交換器晶片所採用的記憶體型式大都是 SDRAM or SGRAM 只有極少數是使用 SSRAM。採用外接記憶體的好處是這些記憶體的容量都相當大，所以可以儲存較多的封包，減少啟動流量控制(Flow Control)的頻率，讓網路傳輸的效率提高。但是相對的也會因此而大幅地增加晶片的接腳數，增加 IC 封裝的成本，以及記憶體供貨的穩定性問題，如此都將會造成系統廠商備料上的困難，進而影響到系統廠商使用此晶片的意願。

嵌入式記憶體(Embedded Memory)

也有的交換器晶片是將封包暫存記憶體改採嵌入式記憶體(Embedded Memory)的方式。它的好處是可以大量地減少晶片的接腳數，降低 IC 封裝的成本並且因為不再須要額外的去採購記憶體，故可以有效地消除系統廠商備料上的困難，另外因為記憶體是在 IC 內部，所以可以較容易的將記憶體匯流排寬度增加，提昇晶片交換資料時的頻寬。它的壞處則是封包暫存記憶體將受到很大的限制。以晶片製程來說，將記憶體整合入交換器晶片當中，目前有採取 SRAM 和 DRAM 兩種不同的製程方式。

Embedded DRAM

整合 DRAM 的優點是其集積度高，相同的單位面積內可以比 SRAM 放入更多的記憶體容量，換句話說相同的記憶體容量，DRAM 所佔的晶片面積(Die Size)會比 SRAM 小的多，但是在與交換器晶片的整合上就需較多層的光罩、製程難度較高且良率較難掌握。

Embedded SRAM

將 SRAM 與交換器晶片整合則製程較易，而且較為容易地去提昇晶片交換資料時的頻寬。它的缺點是集積度會比 DRAM 製程來的差。此外也要注意的是為了儘量減少嵌入記憶體容量，所以採用嵌入記憶體的交換器晶片它在封包的管理上一般是會採取小緩衝區的策略，讓有限的嵌入記憶體容量能夠處理最多的封包數。Gigabit (1000M) Switch Hub Chip 因為需要很大的記憶體頻寬，所以目前 Gigabit Switch 的 Packet Buffer Memory 大都是採用 Embedded SRAM 的架構。原因是它可以利用 Pipeline SRAM 的技術來提高記憶體使用的頻寬。

新技術的支援：QoS

有些廠商強調它們的交換器晶片能夠支援 IEEE 802.1p 的 QoS(Quality of Service)的功能，以符合 VoIP(Voice over IP)、Video Conference、虛擬實境(Virtual Reality)、等須要

封包能夠即時傳送的網路多媒體應用的要求。也就是說 Switch Hub Chip 中支援 Priority Queue, 能夠優先處理權限較高的封包, 藉以消弭訊號延遲的情形。

Virtual LAN (VLAN)

目前大部份的交換器晶片都已經支援了 VLAN 的功能, 但是目前國內廠商大都只支援到較為簡單的 Port based VLAN。較複雜的 MAC based VLAN、Police based VLAN 等都還沒有支援, 因為這些必須要處理到封包當中的 VLAN tag field, 例如必須在晶片內部建立及維護一個 VLAN Port 對映表, 還要能夠從封包中拿除或插入 VLAN tag。這些工作都將會增加晶片設計上的複雜度。表一 我們列出在各種功能採用不同技術來實現的 8 Port 交換式集線器晶片的型號, 以及它們之間基本功能的比較, 藉此說明目前 Layer 2 交換式集線器晶片技術發展的概況。

Vender	Product Name	Ports	Packet Buffer	PHY	Address Table	Trunking	VLAN	QoS	MIB
BROADCOM	BCM5318	8	Embedded 256 Kbyte SRAM	Internal 10M/100M	4K MAC address entries	No	No	No	Yes
ALLAYER	AL104	8	External 8M/16M SGRAM	External 10M/100M RMII PHY	1K MAC address entries	Yes	Yes	No	No
BROADCOM	BCM5680	8	Embedded 512 Kbyte SRAM	External 10/100/1000M	8K MAC + 2K IP address entries	Yes	YES	4 CoS Queue	No
REALTEK	RTL8308B	8	256 Kbyte Embedded DRAM	External 10M/100M RMII PHY	8 K MAC address entries and 128 entries of CAM	No	No	No	No

表一 8 Port 交換式集線器晶片

3. 網路核心設備(Core Device) 中所使用的 ASIC 元件

網路核心設備包括路由器, Layer 3 Switch HUB 等, 主要功能是要決定載送資料的封包(Packet)的傳送路徑(Routing Path)以及處理網際網路上的通訊協定。

這一類設備大都是由 General Purpose CPU 加上專門處理封包的 ASIC 所組成, 以往這些設備當中所使用到 ASIC 很多是屬於所謂的 In house ASIC。也就是某家系統廠商會為了自己的需求而去開發自己專屬規格的 ASIC, 一般這種 ASIC 都是不對外販賣的。如 Netscreen 公司[6], 在它的 Firewall Device 中使用了一顆 GigaScreen Security ASIC 來加速封包的處理及加/解密的功能。但是因為 ASIC 的開發成本相當昂貴, 為了反映研發成本, 所以傳統上網路核心設備的單價也就居高不下。

近年來拜網際網路風行之賜, 網路核心設備的需求量大增, 很多新興的公司想要開發網路核心設備卻苦於沒有 ASIC 可以使用。許多的 ASIC Design House 看準了這個市場的潛力紛紛投入去開發這一類的 ASIC。我們大致上將它們分為路由表查詢晶片, Multilayer Switch 晶片以及目前很熱門的網路處理器(Network Processor)。表二整理這些產品的規格。

3.1 路由表查詢晶片

路由表的查詢為 Router 效能的瓶頸所在，路由表查詢晶片的出現就是利用的 ASIC 的方式來代替軟體查詢，以加速路由表的搜尋。

CAM (Content Addressable Memory) Based 的路由查表輔助晶片

NetLogic 和 IDT[7]等公司都有這類的晶片在販賣，我們以 IDT 的 75T43100 來說明。75T43100 的 CAM 記憶體容量有 32K x 72 bits，可以記錄到 32K 個 entries，它的動作原理是先將 Routing Table 中有關於 IP Routing 所須要的資料例如 IP Address 及 Subnet Mask 等資料一起記錄在 CAM 當中。當要搜尋路由時就將 IP Header 中的相關資訊輸入到此晶片的 Request Bus，得到一個指向 Next Hub Address 記錄的 Index，再藉由此 Index 到外接的 SRAM 中將 Next Hub Address 讀出來送給 ASIC 來使用。它搜尋的速度可以達到每秒 6 千 6 百萬筆路由資訊。一顆晶片大約要 USD\$100。

3.2 Multilayer Switching Engine

目前這類的晶片大都還是由國外網路大廠來提供例如 Allayer[8]、Broadcom、Marvell[9] 等等，一般來說這些晶片都包含 Routing Table search engine、QoS queue management、packet classification、L3/L4 checksum re-calculate 等功能，例如 Allayer 的 AL3000 IP Frame Routing Processor 就可以透過 RoX-II Bus 連接 32 個 Fast Ethernet Ports 或是 兩個 Gigabit Ethernet ports 構成一個 Layer 3 Switch HUB。和 CAM Based 的路由查表輔助晶片不同的是它利用硬體電路方式來實現路由表查表演算法，然後將路由表的資料記錄在 SGRAM/SDRAM 當中，它最大的優點是利用 SDRAM/SGRAM 的價格便宜的優勢來大量增加記錄 IP Routing 的筆數。以 AL3000 為例就可以記錄到 131,072 筆 individual host route entries。

Vender	Product Name	Miscellaneous
Allayer	AL3000 IP Frame Routing Processor	Routing search engine Packet parser engine 802.1q and four QoS Queue NAT Up to 131,072 host route entries Re-assigns VLAN tag and priority for each routed frame External 8MB SDRAM for search 2MB SGRAM for packet queue
IDT	75T43100 IP Co-Processor	Embedded 32K x 72-bit CAM 36/72/144/288 multiple width lookup SSRAM Interface
Netlogic	NL877313 IPCAM-3	64K x 72 bit or 32K x 144 bit or 16K x 288 bit CAM
Samsung	KS32c50100 (SOHO Network Processor)	Embedded ARM 7 One 10/100M Ethernet MAC
Conexant	CX82100 (SOHO Network Processor)	Embedded ARM 940T (144 MHz) Two 10/100M Ethernet MAC

Lantronix	DSTni (SOHO Network Processor)	16 bit Turbo 186 (96 MHz) Two 10/100M Ethernet MAC One internal 10/100 Mbps PHY 128 KB embedded SRAM 16 MB of external memory 16 KB ROM 16 bit TCP/IP checksum generator 16 bit random number generator
Motorola	MPC862T	32-bit RISC Processor Ethernet 10 Base-T up to 4 Fast Ethernet ATM Multi-Channel HDLC up to 64

表二 網路核心設備(Core Device) 中所使用的 ASIC 元件

3.3 網路處理器(Network Processor)

又可以分為兩類，一類為 SOHO 用的網路處理器，一類為企業等級用的網路處理器。

3.3.1 SOHO 用的網路處理器晶片

SOHO 用的網路處理器其設計上的概念是將原本在電路板上的各個 IC 元件整合至單一晶片當中。也就是採用所謂的 SoC(System On Chip)架構，如此一來嵌入式微處理器將因為減去了信號通過接腳時造成的時間延遲，使得操作頻率可以大幅地提高，並且可以減化系統廠商生產的流程。最重要的是它可以很容易的將以前在電路板上以外接式 CPU 執行的程式移植至目前以網路處理器製作成的產品上來執行。所以它本質上它還是 General purpose CPU-based 的形式，大部份網路上封包的處理還是得由軟體來執行，直接利用硬體演算法來加速網路封包的處理地方只佔有很少的一部份。

目前在國內，有兩種類型的廠商正在研發 SOHO 用的網路處理器，一種是原本具有 CPU 技術的廠商將 Ethernet 網路功能整合至一顆 SoC 當中，如金麗半導體(RDC)[10]將 RISC CPU、Ethernet MAC 及 Switch Hub 整合至一顆 SoC 當中，另一種是原本具有網路技術的廠商將 CPU 整合至一顆 SoC 當中，如上元科技(ADMtek)[11]的 SOHO Gateway Controller 將 ARM7 / ARM9 RISC CPU 整合至晶片中。

在國外廠商方面，已經有許多廠商如 Samsung、Conexant[12]、Motorola[13]等推出可量產的產品。以美商 Conexant System Inc 推出的 CX82100 SOHO 網路處理器為例，其內建有一組 ARM 940T 144 MHz RISC CPU，並擁有 2 組 802.3 媒體存取控制器(MAC)、2 組符合業界標準的媒體獨立介面(MII)/七組線路(7W)、一套 USB 介面、一套專屬程式記憶體匯流排、一組擴充匯流排、一組聯合測試協會(JTAG)介面、以及多套時脈與一般用途 IOs(GPIO)。這樣的架構能夠讓製造商將這款裝置透過 MII/7W 介面連結至任何 PHY 元件，再經由 Embedded CPU 執行不同的網路應用程式，就可以讓系統製造商很有彈性的設計出不同的網路產品。

3.3.2 企業或骨幹等級用的網路處理器

此類的網路處理器主要的市場是在於企業使用的網路設備、廣域網路的交換設備、甚至骨幹網路以及電信核心網路的產品，這些設備的傳輸速度已經由每秒百萬位元(Mega)等級進入 Giga 等級，它所需要的是一個具有可程式控制封包分類能力以及具有

高速查表能力的晶片。並且要能夠處理第三層到第四層甚至更高層的通訊協定的封包的交換，分類及路由的決定。此類的網路處理器一般都內含有兩種不同型式的微處理器一起工作，這樣分工的理由是因為可以把 data-plane 及 control-plane 兩種不同特性的封包分別由不同的 CPU 來處理， data-plane packet 需要快速的路徑， control-plane packet 只需要較慢速的路徑就可以了，需要快速路徑的操作包括 classification， lookups or priority checking 等功能，它們需要對於每一個封包的處理都能夠達到 wire speed 的要求。所以在網路處理器晶片當中會有特別的微引擎(Microengine)來加速這類封包的處理，另外對屬於 control-plane 的封包因為其資料量不會太大，所以為了兼顧彈性一般網路處理器晶片會將此部份交由一通用型 CPU(general-purpose CPU)來處理。

目前這類的晶片大都是由國外的廠商來提供，如 Intel[14]、MMC[15]、IBM[16]等。以英特爾(Intel)推出的 IntelIXP1200 網路處理器為例，它就配備有高速的 32-bits StrongARM 嵌入式處理器來處理 control-plane 的封包，並且可以透過 32 bit PCI 匯流排，快取記憶體(Cache)與外部溝通，此外，每個 IXP1200 內部含有 6 個 32-bit 多線程 (Multithreaded) RISC 微引擎(Micro-engine)來處理 data-plane 的封包，能夠對封包承載的資料進行 bit、byte、word、longword 等操作。這 6 個微引擎他們是各自獨立運作的，但彼此之間也可以透過記憶體或暫存器互換資訊，其吞吐量(throughput)可以達到每秒鐘處理超過三百萬個 Ethernet 封包。表三比較市場上幾個網路處理器。

Vender	Product Name	Data-Plane CPU	Control-Plane CPU	Miscellaneous
Intel	IXP1200	6 Micro-Engine	StrongARM	SDRAM up to 256MB SRAM up to 8MB ROM up to 8MB PCI Bus IX Bus
C-PORT	C-5	16 Channel Processor(contains a 32 bits RISC Core + dual parallel Serial Data Processor)	Executive Processor (RISC)	Buffer Memory Size up to 128MB Table Lookup Memory up to 16MB Up to 512 Queues 10Mb Ethernet (RMII) 100Mb Ethernet (RMII) 1Gb Ethernet (GMII and TBI) OC-3c OC-12/OC-12c OC-48 T1/E1 T3/E3 32 bits 33/66Mhz PCI bus serial PROM interface
MMC	NP7120	Packet transform engine Policy engine Statistic engine	Multi-tasking Processor 64-bits	Dual port Gigabit Ethernet packet processor
IBM	PowerNP NP4GS3	16 picoprocessors providing 2128 MIPS	IBM PowerPC	40 Fast Ethernet / 4 Gb MACs OC-48c, OC48, four OC-12, sixteen OC-3

表三 網路處理器規格比較表

4. 網路服務設備(Service Device) 中所使用的 ASIC 元件

網路服務設備主要包含了各式各樣的伺服器(Server)及防火牆(Firewall)，這些網路設備有些是利用個人電腦作為一個平台，在上面執行特定的軟體就變化出不同功能的設備，例如 Mail Server，Web Server，Printer Server，Firewall 等等。也有一些廠商直接將整個系統做在一塊電路板上，在上面執行自己的作業系統及軟體，得到的好處是可以不受個人電腦作業系統的限制，發展出具有自己特色的產品，另外，成本可以更低。不管是上述那一種型式的產品，當它的系統複雜度提高時都必須靠 ASIC 來加速網路的處理。這類的 ASIC 可概分為網際網路處理器(Internet Processor)及網路安全晶片(Security Processor)兩種。

4.1 網際網路處理器(Internet Processor)

網際網路上所使用的通訊協定是 TCP/IP，一些 ASIC 廠商針對 TCP/IP 的特性開發出以硬體方式來處理網際網路通訊協定的晶片。包括有 TCP、UDP、ICMP、ARP、DHCP 等協定，它提供存取界面讓 CPU 可以透過暫存器控制的方式下達建立或移除 TCP/UDP 連線的命令，或是讀取目前 TCP/UDP 連線的狀況，並且還可以自動計算/產生 IP 層或 TCP/UDP 層的 Checksum，即將網路第三，四層連線的工作全都交由此單晶片來執行，如此一來將可讓大幅減輕 CPU 在處理網際網路連線時的負荷，相對來說就是提高了網路傳輸時的吞吐量(Throughput)，讓 CPU 有更多的時間去執行更多網際網路高層的應用程式。目前屬於這類的晶片有 Seiko 的 iChip[17]、WIZnet[18]的 i2Chip 等，它們主要針對的市場是資訊家電，行動通訊及個人數位助理等。表四是各家晶片規格的比較表。

Vender	Product Name	CPU	Embedded RAM	Protocol	Miscellaneous
SEIKO	Ichip S7600A TCP/IP Protocol Stack LSI	External X80 or 68000	10K Byte	TCP IP UDP PPP	Intel/Motorola MCU bus Interface two general sockets UART interface
Wiznet	I2Chip W3100	Embedded 16 bits RISC	24 Kbytes Dual-port SRAM	TCP IP UDP ICMP ARP DHCP	Intel/Motorola MCU bus Interface Four general sockets One MII Interface

表四 Internet Processor

4.2 網路安全加速器 / 處理器晶片(Security Accelerator / Processor)

網路安全晶片可以運用在加解密加速卡或是防火牆設備上做為加解密及認證加速器之用。隨著電子商務的蓬勃發展，SSL 技術已被大部份的 Web Server 及 Browser 廣泛的用來保護線上交易時的資料，SSL 是利用公開金鑰的加密技術(RSA)來做為用戶端與主機端在傳送機密資料時的加密通訊協定。要得到金鑰必須要經過高次方模指數運算(180-bit exponent)。

另外， 虛擬私人網路(Virtual Private Network VPN)， 也是網路安全晶片可以發揮功用的地方， 因為在建立安全的通訊管道時， 必須利用公開金鑰的加密技術來交換金鑰， 在建立連線之後， 必須要利用對稱式加密技術將所有在網路上傳輸的封包的內容都經過加密的處理後傳遞再給對方， 如果將此加密的工作都交由電腦上的軟體來執行， 將會消耗掉大量的 CPU 處理時間， 使用網路安全晶片就可以有效地將 CPU 的負荷轉移至晶片， 節省 CPU 運算的時間。

目前網路安全晶片大都是透過 PCI BUS 和電腦連接， 它動作的程序是 Host CPU 先將封包資料或 Key Setup 資訊存在系統記憶體中， 再將指向定義這些封包和 Key Setup 資訊的結構的指標傳給晶片， 晶片就可以藉由這個指標去取得資料來加密封包或產生金鑰， 完成處理後再經由中斷呼叫的方式將處理狀況回報給 Host CPU 知道， 加密過的資料可以再經由 PCI BUS 送回給 Host CPU， CPU 再去啟動網路處理程式將密文包裝成 TCP/IP 封包後送至目的地。目前的網路安全晶片大都有提供下列以下幾種加解密的功能。

單向雜湊函數

MD5 訊息摘要(Message Digest)是將輸入的任意長度的明文， 壓縮成一個完全唯一的 128 位元密碼。SHA/SHA-1 則是將任意長度的明文處理產生 160 位元的雜湊函數值， 其安全性較高， 但速度較慢。

非對稱式加密

RSA 密碼系統包含金匙的產生， 加密與解密， 強質數的產生等。 要完成這些數學運算需要包括模運算、模乘法運算、模指數運算、模反元素運算、隨機函數產生器等幾個部份。這些運算的數字至少都為數百位元次方的整數， 所以就算已經利用硬體平行處理來加速運算， 還是須要花費數百 ms 的時間才可以計算完畢。

對稱式加密

目前最常用有 DES(Data Encryption Standard)， 3DES 等， 其主要的設計概念是將輸入的原始資料， 我們稱之為明文(plaintext)， 配合金匙一起進行數個回合的排列(permutation)及交換(substitution)等運算， 最後可以得到一筆攪亂的資料， 我們稱之為密文(ciphertext)。再將此密文傳遞給對方， 如果對方擁有相同的金匙則經由相反程序的運算就可得到原始的明文資料。DES(Data Encryption Standard)是由美國國防部於 80 年代制定的資料加密標準。它是一種區塊加密方法， 它將欲加密的信息分割成 64 位元的區

塊，再利用 56 bits 的密鑰加密。由於密鑰長度不長，再加上電腦運算速度愈來愈快，利用窮舉法破解密鑰已非遙不可及的事，其替代方案是採用 3DES，3DES 是利用兩把 56 bit 或三把 56 bits 不同的密鑰利用 DES 演算法將資料連續加密三次，一般相信，使用 3DES 要比 DES 安全得多。但是相對的所花費的時間也較長。

串流式加密

RC2 與 RC4 則是美國 RSA 公司提出的用串流式加密方法，它是屬於對稱式的加密技術，RC2 是用 64 位元的區塊加密，RC4 將密鑰長度變成一個變數，可以隨需要增長密鑰位元，一次計算一個位元組 (byte)。表五 是各家網路安全晶片的型號及基本規格的比較。

Vender	Product Name	Bus	Symmetric Encryption	Key	Hash Algorithm	Public Key Generator	Miscellaneous	Throughput
Hifn	7950 7951	PCI	DES 3-DES RC4		SHA-1 MD5	1536-bits	Compression(LZS and MPPC) Random Number Generator	DES : 134 Mbps
Broadcom	5805	PCI	DES 3-DES		SHA-1 MD5	1024-bits	Randomizer Public Key Accelerator	3DES: 310 Mbps
Philips	VMS747	PCI	DES 3-DES		SHA-1 MD5	1024-bits	ARM7T RISC Randomizer	DES : 492 Mbps

表 五 網路安全晶片的型號及基本功能的比較

5. 結論

本文介紹了三種不同的網路設備中所使用的網路晶片並對晶片規格表上的功能進行技術上的分析，由此我們可以得到網路晶片發展的趨勢，在網路存取設備中使用的晶片將走向高度的垂直/水平整合，就是將 MAC、PHY、Transceiver，三種元件整合至一片晶片上，水平整合是將 SRAM/DRAM 記憶體及更多 Port 數整合至一片晶片上。在網路核心設備中使用的晶片將有兩個走向，往 SOHO 等級使用的晶片將走向系統單晶片 (SoC, System On Chip)，往企業或骨幹等級使用的晶片將走向網路處理器晶片(Network Processor)，它們共同的特徵就是要兼顧系統發展的彈性及網路的效能。在網路服務設備中使用的晶片將更強調對於特定功能的加速性能。

一顆晶片的開發過程是相當煩瑣的，由規格的訂定開始、硬體架構的決定、邏輯電路的設計及驗證、邏輯閘的佈局及繞線、製作光罩、到了晶圓廠生產成爲晶片回來還要再送到封裝廠打線製作成一個顆 IC，最後還要送到測試廠將測試向量都跑過一遍都及格才可以出貨。這些程序所需要的時間及成本都是相當高的，所以在網路的產業當中，系統廠商和 IC 提供廠商之間的關係是非常密切的，爲了減少系統廠商 Design In 的阻力，IC 提供廠商都會將相關的軟體以 Turn-key 的方式提供給系統廠商，同時系統廠商也扮演規格訂定者的角色，在 IC 提供廠商進行新產品開發時就一同參予 IC 開發的工作，這樣良性的互動關係讓 IC 提供廠商設計出來的 IC 能夠符合市場的需要，同時也造就了台灣在網路中低階產品上的地位。

網路是一個充滿想像力的市場，只要有好的構想任何型式的網路晶片都有可能再被開發出來，讓我們大家拭目以待。

參考資料

- [1] http://www.realtek.com.tw/hm/products/cn/rtl8139b_1.htm
- [2] <http://www.asix.com.tw/>
- [3] <http://www.tmi.com.tw/pp-1-all.html>
- [4] <http://www.broadcom.com>
- [5] <http://www.national.com/pf/DP/DP83820.html>
- [6] <http://www.netscreen.com/aboutus/articles/news121399.html>
- [7] http://www.idt.com/products/pages/IP_Co-Processors-75T43100.html
- [8] <http://www.amssv.com/oldallayer/pressrel10.html>
- [9] http://www.marvell.com/Internet/Products/Product_Index/1,2412,2,00.html
- [10] <http://www.rdc.com.tw/>
- [11] <http://www.admtek.com.tw/>
- [12] <http://www.conexant.com/default.sph/SaServletEngine.class/Web/products/index.jsp>
- [13] <http://www.motorola.com/SPS/RISC/smartnetworks/news/presskit/>
- [14] <http://developer.intel.com/design/network/products/npfamily/ixp1200.htm>
- [15] <http://www.mmcnet.com/Solutions/nP7120.asp>
- [16] [http://www-3.ibm.com/chips/techlib/techlib.nsf/techdocs/852569B20050FF778525698F00749CD2/\\$file/NP015700.pdf](http://www-3.ibm.com/chips/techlib/techlib.nsf/techdocs/852569B20050FF778525698F00749CD2/$file/NP015700.pdf)
- [17] <http://www.seiko-usa-eed.com/>
- [18] <http://www.wiznet.co.kr/>