網路監視器之研製

陳惠淳　　伍麗樵

國立雲林科技大學 電子與資訊工程研究所

wuulc@el.yuntech.edu.tw

摘要

本文是討論如何在現今的乙太網路上實作一視窗介面的網路監視器，並利用Window的網路驅動介面規格(NDIS)所提供的功能，來達到控制網路卡及接收子網域上任何的封包。除此之外，我們的網路監視器還能捉取及儲存特定封包，並能將捉取到的TCP/IP封包作格式分析及顯示資料內容的功能，方便網路管理者掌控整個子網域的網路的狀態。

關鍵詞：乙太網路，網路驅動介面規格(NDIS)，網路監視器

1.簡介

科技日新月異，網路的發展速度更是一日千里。在學術網路、HiNet、SeedNet等大力鼓吹網路的便利性之後，無論是個人或公司企業都紛紛急著搭上網路列車。在這樣的一個情形之下，身為一個網路的管理者，如果能夠監視自己的網路，掌握網路的狀態，了解封包傳送情形，取樣封包內容，便能更進一步管理自己的網域，讓網路上的資源能夠做最有效率的使用。

在傳統的EtherNet[4]，封包是以廣播的方式傳送[15]，所以，我們只要在子網域上架設一封包捉取器，就能捉取封包資料並加以分析、統計，以監視此子網域上的封包流量[3, 6]、TCP連接狀態[8-9]、主機資料傳送及接收量，以及相關資料的統計。有這樣的資料統計，便能提供相關的資訊給網路管理者作子網域的管理依據。

本網路監視器的網路環境架構如圖1。監視器架設在host E上，利用EtherNet實體層上的廣播特性及將host E上的網路卡設為完全捉取(PROMISCUOS)模式，監視器即可捉取子網域上的任何封包。

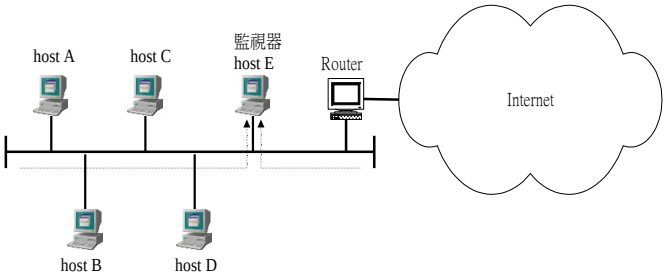

圖1. 網路監視器的網路環境架構圖

我們的網路監視器是架設在Windows的作業系統環境上，以提供圖形化的使

用者介面讓網路管理者更容易操作，也讓管理者更容易了解資料內容。網路監視器的主要功能如下：

1.能監視子網域上封包的流量。例如每秒鐘子網域上有多少個TCP封包在流動，多少個UDP封包在流動。
2.能監視子網域上封包發送情形。例如監視到host A送出了一個200Bytes的TCP封包到子網域上。
3.能記錄網路上Host傳送及接收資料的統計。例如分析host A從開始到目前總共送了多少Bytes的資料。
4.能監視子網域TCP連結情形。例如host B與host C有建立一條TCP的連線。
5.能設定捉取條件，來捉取子網域上的特定封包。例如捉取host C送到host B的封包，並且儲存。
6.可對捉取到的封包進行格式分析。例如分析封包之來源、目地位址和通訊協定。

2.系統架構

在此節中我們對網路監視器的系統架構作一個介紹，分為Network Driver Interface Specification(NDIS)[13-14]，Virtual Device Driver(VxD)[5, 12]及我們研製的網路監視器軟體架構三個部分。圖2所示為我們設計的網路監視器的架構圖，├─形部位為Windows提供的NDIS介面函式庫。虛線所圍部分為我們研製的程式架構，可以分為VxD及Win32應用程式兩個部份。

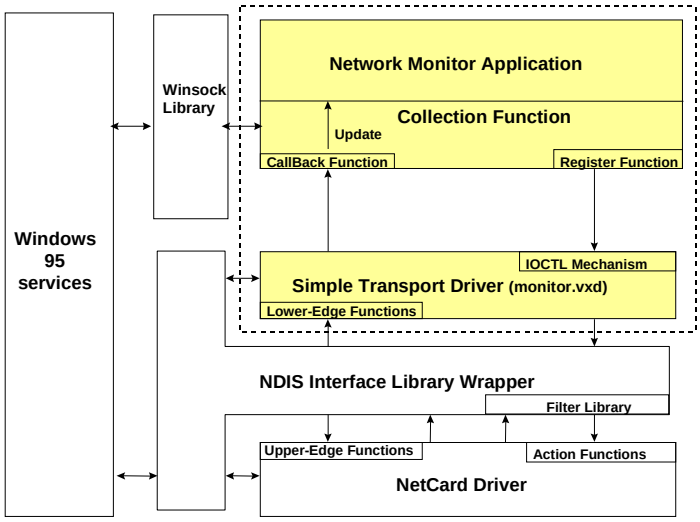

圖2. 網路監視器系統架構圖

2.1 Network Driver Interface Specification (NDIS)

在Windows作業系統的架構中，網路通訊協定層(如TCP/IP)與網路卡之間的通訊均需透過NDIS所定義的介面作通訊，它除了提供網路驅動程式（Network Interface Card driver）與最下層的網路卡（Network Interface Card）溝通的介面，並提供與上層的傳輸層驅動程式（Transport driver）溝通的介面，以及作業系統溝通的介面。NDIS主要的特色有：

1.允許傳輸層驅動程式設定網路驅動程式上的配置參數。
2.允許傳輸層驅動程式查詢網路驅動程式上的配置參數。
3.傳輸層驅動程式可將網路封包（Network Packet）送到任何一個在它下層的網路驅動程式，並由網路

驅動程式送到相連的網路上。

4.網路驅動程式可以用非同步（Asynchronously）的方式將網路上的狀態通知給上層的傳輸層驅動程式。

5.網路驅動程式可由任何一個網路卡上收到一個或多個網路封包，並可將封包送給上層的一個或多個傳輸層驅動程式。

利用查詢及設定網路驅動程式的參數，即可建立一個新的傳輸協定, 而新的傳輸協定和其他協定可平行存在而且不互相干擾。此外NDIS是設計成VxD的型態存在，所以NDIS所提供的函式，並不能直接由Win32應用程式呼叫，必需要由下一節所介紹的VxD來呼叫。

2.2 Virtual Device Driver

在Windows作業系統可以執行三種不同型態的應用程式：DOS 應用程式、Win16及Win32應用程式等。爲了克服執行不同型態的應用程式所產生的障礙，Windows作業系統提供了每種應用程式一個虛擬機器(Virtual Machine)的環境。對應用程式而言，虛擬機器就如同一部真正的機器一般，讓應用程式覺得它擁有整部機器的控制權，但是這是虛擬機器所提供的虛擬假像；可是，當我們想直接控制硬體等低階設備時，就必須藉由Windows所提供的一種控制硬體系統的特殊程式，稱爲虛擬驅動程式（Virtual Device Drivers VxDs），來達到直接控制硬體的目的，在這小節我們將介紹Windows作業系統中的虛擬機器，以及虛擬驅動程式的架構。

虛擬機器環境是一個由系統所產生的假像，Windows作業系統將所有的資源以分時競爭的方式分給所有的應用程式，讓應用程式產生自己擁有整個機器控制權的假像；也就是說，當一個應用程式在執行時，並不考慮系統中是否有其他程式也同樣在執行，而以爲自己是系統中唯一在執行的程式，因此它自然地認爲自己擁有整個機器的控制權。

系統中管理所有虛擬機器的管理者，稱爲虛擬機器管理器（Virtual Machine Manager VMM），需特別注意的是，在Windows作業系統中，所有的Windows應用程式，包括Win16及Win32應用程式，都使用同一個虛擬機器，稱爲系統虛擬機器（System VM），而每個DOS應用程式則有自己獨立的一個虛擬機器，如同之前所說的，虛擬機器是由系統所產生的假像，因此，應用程式無法直接的控制硬體裝置，而必須向Windows作業系統核心層執行的VxD提出要求，來完成想要控制硬體的動作。由於虛擬驅動程式是在Windows作業系統的核心層執行的程式，所以它就如同DOS中的驅動程式一般，可以直接控制與系統相關的資源。

VxD可以含有不同的介面來讓不同類型的程式呼叫。如果我們要在Win32應用程式裏面呼叫某個VxD提供的函式，這個VxD必需提供W32 Device I/O Control

（IOCTL）的介面。而當Win32應用程式呼叫VxD的函式時，必需先用Window API CreateFile()(圖3)來開啓這個VxD。再依據所要呼叫的函式，經由VxD提供的IOCTL介面，使用Window API DeviceIOControl()傳入一個參數資料(DIOCParams)給VxD，而VxD就根據這個介面參數資料來取得WIN32應用程式所欲呼叫的VxD函式，和呼叫這個VxD函式所需的參數值，之後再代替Wind32應用程式呼叫該函式。當Win32應用程式不再使用該Vxd時，再利用Window API CloseHandle()將這個VxD給關閉。圖3爲Win32應用程式與VxD溝通的架構。

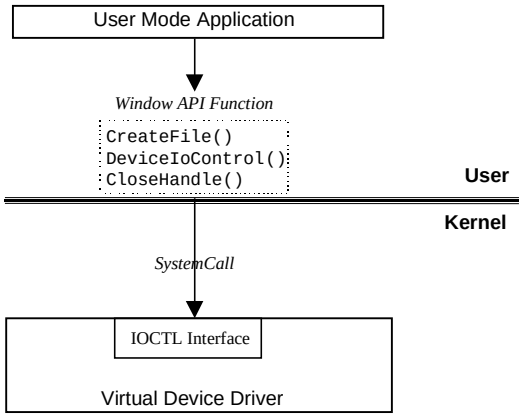

圖3. 應用程式與VxD的溝通介面

2.3 軟體架構

我們是在Windows95作業系統發展我們的網路監視器，分爲Win32應用程式及VxD(monitor.vxd)兩部分。應用程式經由IOCTL介面向monitor.vxd提出要求，再由monitor.vxd配合圖2向網路卡提出要求，並將得到的回應向上傳回給應用程式(如圖2所示)。

利用每個傳輸層都可向NDIS設定個人接收型態的特性，我們的監視傳輸層(monitor.vxd)向NDIS註冊過後，便將其接收型態設定爲完全捉取(PROMISCUOS)，換句話說就是說不管流經過網路卡的封包目地位址爲何，網路卡都會把所有流過的封包捉取起來。網路卡在捉到封包之後即把封包送往NDIS，NDIS再呼叫上層註冊過的傳輸層monitor.vxd來捉取封包資料。監視傳輸層monitor.vxd在捉取完封包資料後，再呼叫應用程式來捉取資料；當應用程式取得資料後，便進行資料儲存、分析及顯示的工作。

在應用程式方面，採用MDI(Multiple Document Interface)的架構，也就是在主程式裏可以將同樣的一份資料以多種不同的子視窗顯示。在應用程式收到由監視傳輸層的資料後，每個不同的Active子視窗便依照其設定將同一份資料作不同分析，儲存及顯示，而Inactive的子視窗，則不作任何分析動作，以增加系統處理效率。

3.實作成果

我們所設計的監視器畫面如圖4，從主畫面中，管理者即可觀看到監視器所在的子網域上的網路封包流量(圖5)。利用主畫面上的工具列可開啓或關閉其他的功能視窗，以監視網路封包發送的情形(圖6)，顯示子網域TCP的連接狀態(圖7)，統計子網域上各主機的資料發送及接

收的數目(圖8)，更可設定條件來捉取特定的封包(圖9)，並顯示其封包的內容(圖10)及TCP/IP封包格式分析視窗(圖11)。

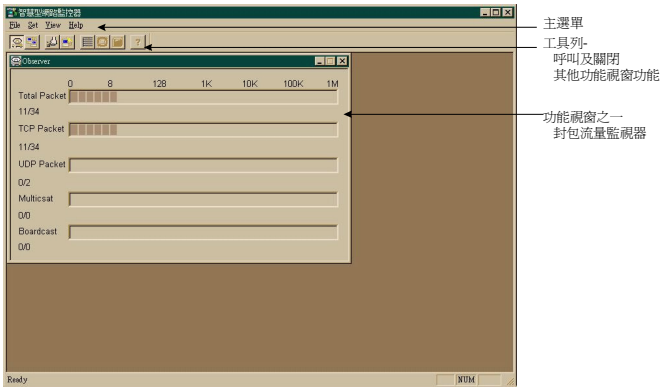

圖4. 網路監視器主畫面

3.1 網路封包流量監視視窗

顯示每秒鐘各種封包的流量(packets/sec)，主要有TCP packet數、UDP packet數、Multicast packet數、Broadcast packet數等。圖5裏的24/176等數字表示的意思爲目前流量/曾經出現過的最大量。

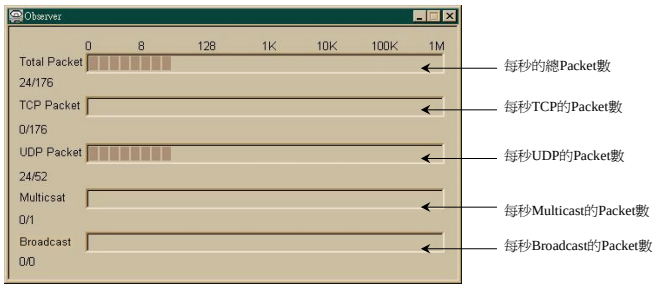

圖5. 網路封包流量監視視窗

3.2 子網域封包發送視窗

可記錄封包發送者及接收者的IP位址、封包發送者及接收者的port number、使用的協定名稱、封包大小、及記錄監視到此封包的時間。

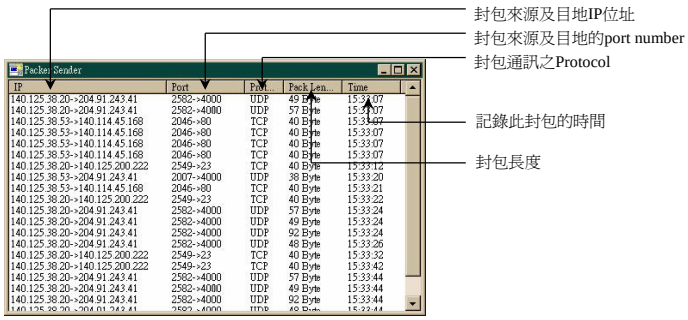

圖6. 子網域封包發送視窗

3.3 TCP連接狀態顯示視窗

可以判斷子網域上TCP連接情形，並顯示連接關係及開始監視時之時間。

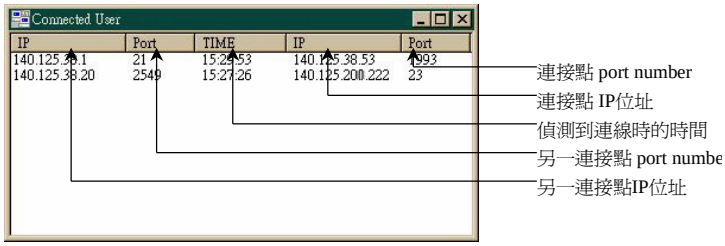

圖7 . TCP連接狀態顯示視窗

3.4 子網域上主機傳送接收資料統計視窗

可以統計網路主機的傳送及接收的資料位元數，並記錄其最新一筆傳送或接收資料的相關資訊。

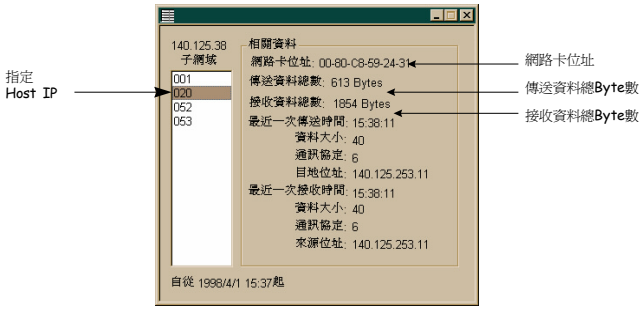

圖8. 子網域上主機傳送接收資料統計視窗

3.5 封包捉取視窗

可以設定捉取的條件來捉取子網域上流過之封包，捉取條件最多可設定五組，並可開啓封包資料視窗(圖10)觀看所捉取到之封包的資料。

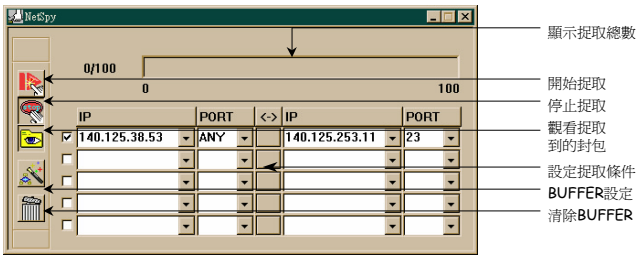

圖9. 封包捉取視窗

3.6 封包資料顯示視窗

經由封包捉取視窗所開啓的視窗，可顯示封包相關資料及封包Binary資料和ASCII資料。在封包編號上雙擊滑鼠左鍵可開啓封包格式分析視窗(圖11)。

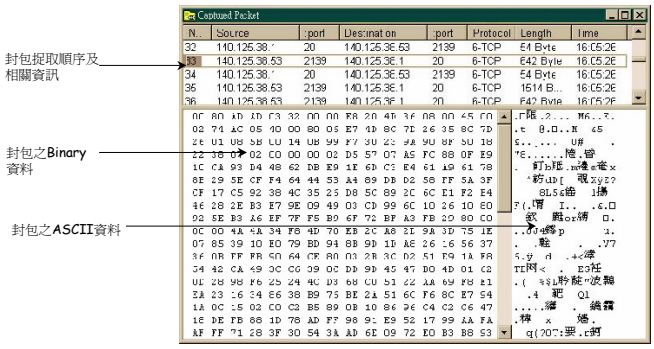

圖10. 封包資料顯示視窗

3.7 TCP/IP封包格式分析視窗

可分析被捉取的TCP/IP封包格式[3,6,7-10]，並將Binary資料轉換成對應的協定內容，讓使用者更容易了解封包結構。

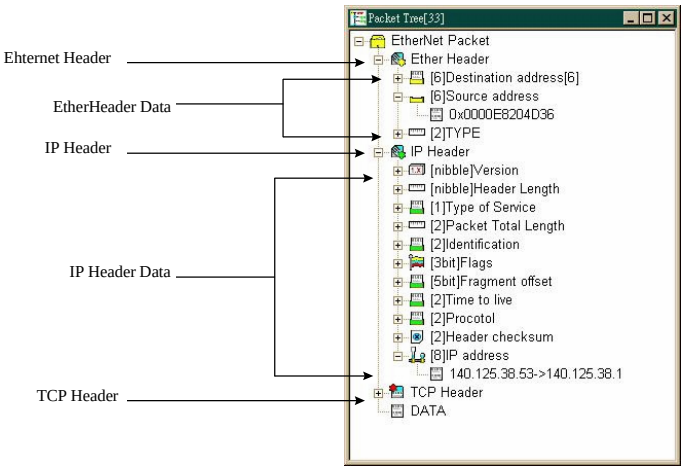

圖11. TCP/IP封包格式分析視窗

4.結論

現在市面上的網路監視器有很多種類，但各有其優缺點，如Triticom的EtherVision提供有traffic monitoring，network event logging，variety of alarms等功能，但是只有簡易的視窗化使用者介面，而且只能在DOS上執行。Frye Utilities是NetWare的Monitor只能提供監視Novell網路狀態的功能。NetXray提供了視窗化的操作介面，且在捉取特定封包功能上，也有較佳的捉取條件設定功能，但價錢卻是非常的昂貴。

我們的視窗化網路監視器，能幫助網路管理者更容易的了解到網路上的狀態、監視網路有無怪異資料量之傳送，特定封包捉取的功能更能鎖定疑似非法的主機所傳送的封包。在我們特有的封包分析視窗中，雖然目前只能分析TCP及UDP的封包，未來將會增加其他格式封包的分析功能；此外並還加強本網路監視器的Performance及分析Lost rate，期望使該監視器的應用更爲廣泛。

參考資料

1. B.Quinn, D. Shute , *Windows Sockets Network Programming* , Addison Wesley
2. D.Ralph , Win32 Network Programming , Addison-Wesley
3. D.Hornig, ”Standard for the Transmission of IP Datagrams over Ethernet Networks,” 1984,RFC 894
4. G. Held, *Ethernet Networks*, Wiely
5. H.Karen, *Writing Windows VxDs and Device Drivers* , (1997),R&D Books
6. J.b. Postel, J.K. Reynolds, “Standard for the Transmission of IP Datagram over IEEE 802 Networks, “ 1988, RFC 1042
7. J. Postel, “User Datagram Protocol,” 1980,RFC 768
8. J. Postel, “Transmission Control Protocol,” 1981,RFC 793
9. W.Richard Stevens , *TCP/IP Illustrated, Volume1*,Addison Wesley
10. W.Richard Stevens , *TCP/IP Illustrated, Volume2*,Addison Wesley
11. W. Oney, *Systems Programming for Window95,* Microsoft Press
12. S. Dhawan, *Networking Device Drivers*, VNR Communications Library
13. *Network Guide for Windows 95 DDK* , (1995), Microsoft com
14. *Network Reference for Windows 95 DDK* , (1995), Microsoft com
15. 黃能富,*區域網路與高速網路*,維科出版社
16. 陳惠淳,陳世仁,伍麗樵,”智慧型網路監控器之研製,” 國立雲林科技大學技術報告, Taiwan, R.O.C.