イーサネット及びTCP／IPパケットモニタの試作

北陸職業能力開発大学校　平野昭男

Trial rearing of Ethernet and TCP／IP packet monitor

Akio HIRANO

要約　イーサネット及びTCP／IP通信プロトコル等の原理を理解する事はネットワーク技術を習得する上において不可欠である。しかし、入門者や学生にとってはこれらの知識、技術は抽象度が高く、教科書等での学習を通してもなかなか理解し難いのが実情ではなかろうか。

この解決策の一つとして、ネットワークアナライザ等を用いてパケット解析等を行ない出来るだけ具象的な観点から学習を進める事である。今回、このような考え方に基づいてVisual Basic言語、及び市販のネットワークボードを用いてネットワークモニタを開発し、これを用いてイーサネット及びTCP／IP通信プロトコルに関する教育訓練を試行してみた。

Ⅰ　はじめに

ネットワークで用いられる通信プロトコルとしてリンク層やネットワーク層及びトランスポート層では主としてイーサネットやTCP／IPプロトコルが、セッション層以上ではHTTP，SMTP，POP3、TELNET、FTP等のプロトコルが用いられている。HTTPやSMTP，POP3等のプロトコルはインターネットやE-mailのアクセス時に直接関わり、日常的に使用しているためにおおよその動きをつかむことが出来る。しかし、イーサネットやTCP／IPプロトコルは表面に現れずバックグランドで動作しているため、ネットワークの骨格をなす重要なプロトコルであるにも関わらずその詳細な動きまでなかなか把握出来ないのが実情ではなかろうか。

そこで筆者はこれまでにこれら下位層のプロトコルの習得を補助する目的でMS-DOSのOS上で動作するイーサネット及びTCP／IPパケットモニタを作成し、これを用いてパケット解析実習等を能力開発セミナ等で実施してきた。

MS-DOS上で動作するパケットモニタはC言語で記述していたが、今回プログラム開発言語にVisual Basicを用い、Windows OSの環境で動作するパケットモニタを作成した。

能力開発セミナで試用してみてMS-DOS上で動作するパケットモニタに比べ操作性、視覚性が格段に改善され、実習機材としての有用性が確認できたので作成したパケットモニタの開発方法やその機能等について報告する。

Ⅱ　使用するLANボードの概要

ここではイーサネットネットワークコントローラとしてナショナルセミコンダクタ社製のDP8390を搭載したLANボードを用いる。このコントローラを搭載したLANボードとしてDOS／V用としてはLD-PNE20／T、PC98用としてB4680インタフェースボードT等がある。

これらのLANボードを用いてパケットの受信を行なう場合、まず受信したパケットは一旦LANボード上のRAMにバッファリングされる。同時に割り込み

論文受付日　H12.11.30

ステータスレジスタの受信割り込みビットPRXがアクテーブになるので、このビットを監視し、パケットの受信が確認されればバッファ上のパケットをホストCPUに転送する。受信バッファは図2のようにRAMの受信バッファの先端と終端が連結されており、エンドレスなリングバッファとして構成されている。

このため、ホストCPUの負荷が多い場合でも受信データの取りこぼしが生じないように工夫されている。また、受信バッファは256バイトを1ページとするページ単位で管理されており、受信パケットの長さが1ページのバイト数に満たない場合でも、次ぎに受信するパケットは次ぎのページからバッファリングされる。一方、パケットの送信を行なう場合は、まずホストコンピュータ上でイーサネットアドレスを含む全ての送信データを作成し、このデータをLANボード上のRAMに転送し、DP8390のコマンドレジスタのTXPビットをアクテーブにする事によりRAM上の送信データがイーサネットの送信アルゴリズムに従ってラインに送出される。

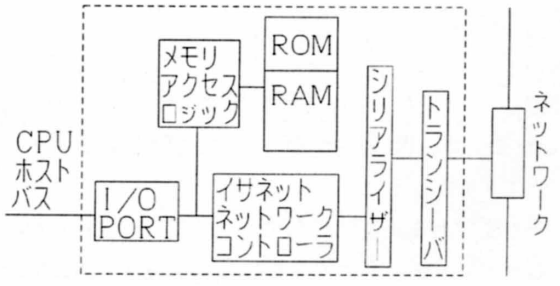

図1　イーサネットLANボードの構成概要

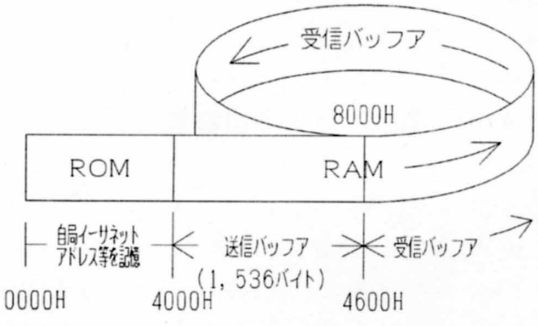

図2　LANボード上のメモリー構成

また、LANボードのアクセスは全てI/Oポートを通して行なわれる。

LANボードのI/OアドレスはAT互換機では通常300(H)～31F(H)番地におかれる。

これらのLANボードは通常Windows OSの環境下ではプラグ&プレイバイスとして認識されるが、これらのLANボードに付属してくる環境設定ソフトを用いてその動作モードを“ジャンパーレス”モードに設定する事によりWindows OSの管理から開放され、ユーザが作成した制御プログラムによって自由に制御できるようになる。

Ⅲ　LANボード制御プログラム

1．制御プログラム開発の基本的な要素

本来、LANボードのドライバソフト等の制御プログラムは動作の高速性を保証するためにアセンブリ言語で記述されるが、コンピュータ上で同時に実行されるタスクの数が限定されていれば高級言語で制御プログラムを記述しても速度的には全く支障なく動作する。ここでは開発の容易さを考慮しVisual Basic言語を用いる。

Windows95／98では直接入出力ポートをアクセスする命令として、出力命令（_outp)、入力命令(_inp）の使用が許可されている。この命令を用いる事により容易にLANボードの制御を行なう事ができる。しかし、これらの命令はVisual Basic上からは直接呼び出す事が出来ないため、Visual C＋＋等を用いて入出力命令をサポートするDLLファイルを作成する必要がある。Visual Basicからは作成したDLLファイルを用いて間接的に入出力命令を呼び出す。

また、DP8390には80近くのレジスタが存在し、これらのレジスタを目的に応じてアクセスしてパケットの送受信を行なう。

ところで、DP8390は送信、受信バッファRAMをホストコンピュータのメモリーアドレスの一部にマッピングするローカルDMA方式とLANボード上で独立にメモリー空間を確保するリモートDMA方式をサポートしている。最近は殆どのLANボードはリモートDMA方式を採用しているが、この方式はLANボード上でRAMが割り付けられているアドレスを直接アクセスするのではなく、特定の入出力ポートを通して間接的にRAMをアクセスする。入出力ポートを1回アクセスする毎にRAMをアクセスする実効アドレスは1づつインクリメントされる。これらの事柄を理解してパケットモニタプログラムを作成する。

2．基本的なLANボード制御プログラム

各種のパケットモニタプログラムを開発する上で共

通的にプログラミングを必要とする部分について記述する。

まず、使用するLANボードに割り付けられているイーサネットアドレスは図2に示すようにROMの0000番地から0011番地に書き込まれている。このイーサネットアドレスを読み出し、DP8390のPhysical レジスタに書き込む事によってLANボードは初めて固有のイーサネットアドレスを保有することになる。その設定プログラム例を図3に示す。

次ぎに、パケットを受信するための基本的なプログラムの例を図6に示す。初めに、リモートDMA並びにRAMの受信バッファ領域をリングバッファ構成とするための各種のレジスタの設定及び受信モードや割り込み関係のレジスタの初期化を行なう。

パケットの読み出しルーチンはタイマーコントロールを用いて100mS位毎に受信割り込みビットPRXをセンスし、このビットがアクテーブになっていれば1パケットずつ読み出しホストコンピュータに転送する。パケットを読み出した後は次ぎのパケットを受信するためにリモートDMA、リングバッファ関係のレジスタ類を再設定する。

```
Dim i As Integer
Dim RD As Integer
Dim MyEtherAdr(6) As Integer
    ' リモートDMAリードモード
outportb &H300, &HA
    ' バイト幅DMA転送モード
outportb &H30E, &H58
    ' リモートDMAスタートアドレス下位バイト
outportb &H308, &H00
    ' リモートDMAスタートアドレス上位バイト
outportb &H309, &H00
    ' ROMから読み出す下位バイト数
outportb &H30A, 12
    ' ROMから読み出す上位バイト数
outportb &H30B, 00
    ' ROMから自局イーサネットアドレスを読み出す
For i=0 To 11
 RD=inportb(&H310)
 If ( i Mod 2 )=0 Then
    MyEtherAdr(i/2)=RD
 End If
Next i
  ' DP8390のページ1のレジスタ群を選択
outportb &H300, &4A
  ' Physical アドレス レジスタに
    自局イーサネットアドレスを書き込む
For i=0 To 5
  outportb &H301+i, MyEtherAdr(i)
Next i
  ' DP8390のページ0のレジスタ群を選択
outportb &H300, &HA
```

図3　自局イーサネットアドレスの読み出し

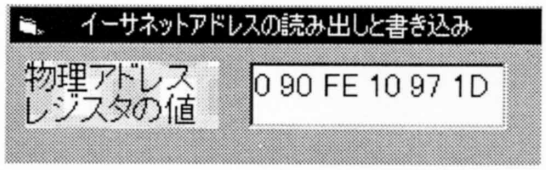

図4　図3に基づいて作成した自局イーサネットアドレス読み出しプログラムの実行例

図5　図6に基づいて作成したイーサネットパケットモニタの実行例

Ⅳ　制作したモニタプログラム

基本的なパケット受信プログラム等を用いて下記のようなネットワークモニタプログラムを作成し、セミナ等の実習教材として利用している。

- イーサネットパケットモニタ（図5）
- 一定の時間を定めてモニタしたイーサネットパケットのヘッダ部の表示(図8)
- ARPパケットのモニタ（図10）
- TCP／IPパケットのモニタ（図12）

これ以外にリンク層でのパケットの送受信プログラムを作成し、基本的なイーサネットの通信原理についても実習を行なうようにしている。

1．　一定の時間内にネットワークを流れるイーサネットパケットのモニタ

イーサネットでは基本的に図7に示すパケットフレームを用いてリンク層での通信が行なわれる。このため、上位層のプロトコルを理解する前にまずイーサネットパケットフレームの働きを理解する必要がある。

作成したイーサネットパケットモニタではネットワークを一定の時間モニタし、その間に流れるパケットを受信し、受信したパケットをホストコンピュータのメモリにバッファリングした後、ヘッダのみを取り出し

```
            〉
＊＊＊　各種レジスタの初期化　＊＊＊
   ' 受信スタートページ
outportb &H301, &H46
   ' 受信ストップページ
outportb &H302 &H80
   ' Boundaryポインタ設定
outportb &H303, &H46
   ' 1ページ目選択
outportb &H300, &H4A
   ' カーレントページレジスタ設定
outportb &H307, &H46
   ' 0ページ目選択
outportb &h300, &HA
   ' バイト幅DMA転送
outportb &H30E, &H58
   ' 割り込みレジスタリセット
outportb &H307, &HFF
   ' 割り込みマスクレジスタクリア
outportb &H30F, &H0
   ' 受信コンフィギュレーションレジスタセット
outportb &H30C, &H1F
   ' RAM受信バッファ先頭アドレスLowバイト
outportb &H308, &H0
   ' RAM受信バッファ先頭アドレスHeightバイト
outportb &H309, CurrentPage
--------------------------------
＊＊＊　RAM受信バッファの初め4バイトは　＊＊＊
      DP8390によって付加された情
      報である
   ' 受信状態
ReceiveStatus=inportb(&H310)
   ' 次ぎのパケットの格納ページ
ReceiveNextPage=inportb(&H310)
   ' リングバッファを構成するための変数に次ページを代入
NextPkt=ReceiveNextPage
   ' 受信Lowバイト
ReceiveByteLow=inportb(&H310)
   ' 受信Heightバイト
ReceiveByteHeight=inportb(&h310)
   ' Boundary Pointerの設定
     (注) DP8390取説参照
If (NextPkt-1)<&H46 Then
   outportb &H300, &HA
   outportb &H303, &H7F
End If
outportb &H303, NextPkt-1
--------------------------------
＊＊＊　1パケットの読み出し　＊＊＊
   ' イーサネット宛先アドレスの読み出し
For i=0 to 5
   DistnatinEtherAdr=inportb(&H310)
Next i
   ' イーサネット発信元アドレスの読み出し
For i=0 to 5
   SoyceEtherAdr=inportb(&H310)
Next i
   ' イーサネットタイプの読み出し
For i=0 To 1
   EtherNetType=inportb(&h310)
Next i
   ' リンク層におけるデータの読み出し
NL=ReceiveByteLow-18
NH=ReceiveByteHeight
outportb &H30A, NL
outportb &H30B, NH
ReadCount=NH*256+NL
For i=0 To ReadCount
   RD=inportb(&H310)
Next i
--------------------------------
  ＊＊＊　パケットリード後の処理　＊＊＊
   ' CurrentPage>StopPage の時の処理
If CurrentPage >=&H80 Then
   CurrentPage=&H46
   outportb &H307, CurrentPage
   outportb &H300, &H300, &HA
End If
   ' 次ぎのパケットの格納ページをセット
outportb &H308, &H0
outportb &H309, CurrentPage
   ' 受信割り込み等の許可
outportb &H307, &HFF
outportb &H30F, &H0
            〉
```

図6　パケット受信基本プログラム

て表示している。図8はプログラムを実行した時のモニタリングの例である。(モニタ例ではブロードキャストパケットのみがモニタされている。これは他のノード宛てのパケットがラインに挿入されているルータによって遮断されているためと考えられる)

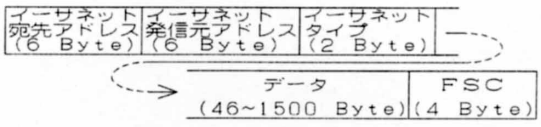

図7　リンク層におけるイーサネットのパケットフレーム

図8　図7に基づいて作成したイーサネットパケットのヘッダ部のモニタ

2．ARPパケットのモニタ

ARPは通信する相手局のイーサネットアドレスが不明の場合にそのイーサネットアドレスを探索するためのパケットである。初めに探索する相手局のIPアドレスをブロードキャストする。該当するノードは自局のイーサネットアドレスをARPパケットに書き込んで発信局に送り返してやる。このように通信局双方のイーサネットアドレスが判明して初めて通信が可能となる。

ARPパケットは構造が簡単ではあるがその仕掛けが巧妙であり、パケット解析の教材として是非取り上げたい題材である。(図10では相手局のイーサネットアドレスが不明であるのでDestination Ethernet Addressの欄は０００００００が書き込まれている)

3．TCP／IPパケットモニタ

TCP／IPパケットはイーサネットフレームのデータ部に書き込まれているので作成したモニタでは図12のようにイーサネットのヘッダからTCPヘッダまで全てを表示するようにしてみた。

IPヘッダの中でヘッダ長が5の場合はオプションとパデングの要素は付加されないので注意を要する。

TCPヘッダをモニタして一番注意を喚起する項目

はTCP Flagであろう。TCPは信頼性のある通信が確保されていると言われるのはこのTCP Flagを用いて図13に示すようなハンドシェーク通信が行なわれているためである。このTCP Flagを観察する事によりハンドシェークの流れを理解する糸口が得られるものと考えられる。また、TCPでは相手局の応答を待たずに連続して複数のパケットを連続的に伝送できるいわゆるウインドウ制御が行なわれている。こられの機能を理解するためにTCPの通番、受信確認番号、ウインドウ制御などの項目の解析が役に立つものと思われる。

ハードウェアタイプ	プロトコルタイプ
HLEN	PLEN　オペレーション
発信元イーサネットアドレス	
発信元イーサネットアドレス(続き)	発信元　IP　アドレス
発信元　IP　アドレス(続き)	探索するイーサネットアドレス
探索するイーサネットアドレス続き)	
探索する　IP　アドレス	

図9　ARPパケットのフォーマット

```
ARP（アドレス解決プロトコル）
パケットモニタ

Physical Layer

  Destination EtherNet Address : FF FF FF FF FF FF
  Souce EtherNet Address       : 00 00 85 04 42 E9
  EtherNet Type                : 0806

ARP Layer

  HerdWare                     : 0001   (10Mbps EtherNet)
  protocol                     : 0800
  HLEN                         : 6
  PLEN                         : 4
  Operation                    : 0 1
  Souce EtherNet Address       : 00 00 85 04 42 E9
  Souce IP Address             : 172 16 80 249
  Destination EtherNet Address : 0 0 0 0 0 0
  Destination IP Address       : 172 16 80 190
```

図10　図9に基づいて作成したARPパケットモニタ実行例

V　おわりに

作成したパケットモニタについてその概要を紹介したが、通信プロトコルのフォーマットがわかっていれば比較的容易にパケットモニタの制作が可能である事が認識される。

高価な市販のモニタを使用した場合では一般的にグループ単位の実習となるが、ここで紹介したパケットモニタは安価なLANボードとプログラム制作ソフトのみで開発が可能であるので実習生一人一人が個々に実習を行なう環境が提供でき、実習効果を高める事が可能である。

バージョン Version	ヘッダ長 IHL	サービスの種類 Type of Service	パケット長 Total Length	
フラグメント識別子 Identification			フラグ Flags	フラグメントオフセット Fragment Offset
寿命 TTL		プロトコル Protocol	ヘッダチェックサム Header Checksum	
始点アドレス　Souce　IP Address				
終点アドレス Destination IP Address				
オプション Option				パディング Padding
始点のポート番号 Souce Port			終点のポート番号 Destination Port	
通番 Sequence Number				
受信確認番号 Acknowledgment Number				
データのオフセット Data Offset	予約済 Reserved	フラグ URG ACK PSH RST SYN FIN	ウインドウ制御 Window	
チェックサム Checksum			緊急ポインタ Urgent Pointer	
オプション（無くても良い） Option				
データ部分　Data				

IPヘッダ　TCPヘッダ

図11　TCP／IPヘッダのフォーマット

```
TCP／IPパケットモニタ
EtherNet Header
    Destnation EtherNet Address : FF FF FF FF FF FF
    Souce EtherNet Address      : 00 10 07 D8 AC 00
    EtherNet Type               : 08 00
IP header
    IP Version                  : 4
    Header Length               : 5
    Type of Service             : 0
    Total Packet Length         : 1 76
    Identification              : 0 0
    Flags                       : 0
    Fragment Offset             : 00
    Time to Live                : 2
    Protocal                    : 17
    Header Check Sum            : 189 131
    Souce IP Address            : 172 16 80 254
    Destination IP Address      : 172 16 80 255
TCP Header
    Souce Port                  : 2 8
    Destination Port            : 2 8
    Sequence Number             : 1 56 0 0
    Acknowledgment Number       : 2 1 0 0
    Data Offset                 : 0
    TCP Flag
        URG=0  ACK=0  PSH=0  RST=0  SYN=1  FIN=0
    Window Control              : 0 0
    Check Sum                   : 172 16
    Urgent Pointer              : 60 0
    TCP Option                  : 0 0 0 0
```

図12　図11に基づいて作成したTCP／IPパケットモニタの実行例

今後の課題としてPing等のICMPプロトコル、インターネット関連の通信プロトコル解析モニタの開発も試みたい。この報告がこれらのモニタの開発を試行される方々にいささかなりとも参考となれば幸いである。

終りに本パケットモニタの制作にあたり種々の情報やLANボードの提供を頂いたナショナルセミコンダクタ・ジャパン社の河西　基文氏、通信プロトコルについて御教授頂いた、水田英介　元職業能力開発大学

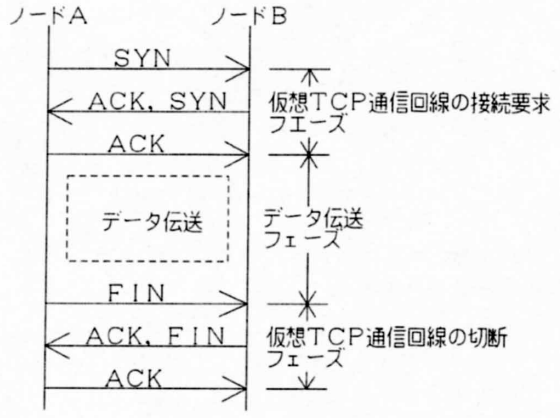

図13 TCPにおけるハンドシェーク通信の例

校・高度ポリテクセンタ教授に衷心よりお礼申し上げたい。

また、日頃貴重な助言を頂いている当校情報技術科職員、並びに、このパケットモニタを開発する初期の段階で卒業研究のテーマとして取り組んでくれた富山職業能力開発短期大学校第19期生、押田 善和君に謝意を表したい。

[参考文献]

(1) ナショナルセミコンダクタ、DP8390シリーズ各種取り扱い説明書、ナショナルセミコンダクタ
(2) アライドテレシス、CentreCOM SICボード技術解説書、アライドテレシス
(3) 船田 悟史、Ethernetカードのハードウェア&ファームウェア、トランジスタ技術1997年7月号
(4) 竹下隆史 他著、マスタリング TCP/IP入門編、オーム社
(5) Philip Miller著、マスタリング TCP/IP応用編、オーム社
(6) Kevin Washburn, Jim Evans著、TCP/IPバイブル、ソフトバンク