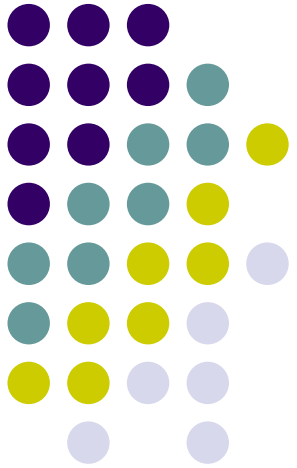
實驗2 乙太網路協定分析

實驗目的：

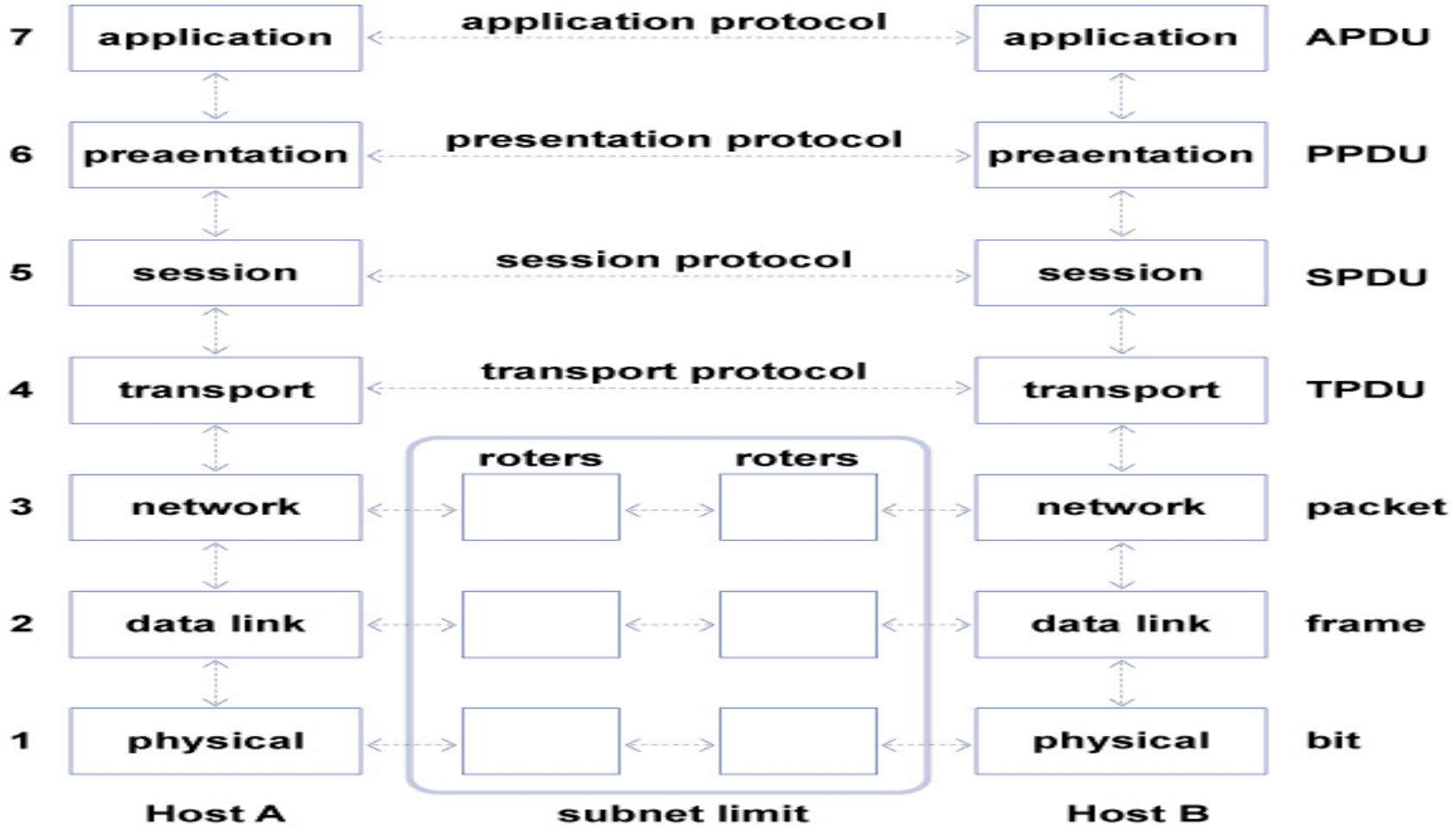
- 明瞭CSMA/CD的工作原理
- 解析乙太網路協定下框架資料傳送的格式



背景資料

- 維基百科（http://zh.wikipedia.org）對乙太網路的說明如下：『乙太網路（Ethernet）是一種電腦區域網組網技術。IEEE制定的IEEE 802.3標準給出了乙太網路的技術標準。它規定了包括物理層的連線、電信號和介質訪問層協議的內容。
- 乙太網路的標準拓撲結構為匯流排型拓撲，但目前的快速乙太網路（100BASE-T、1000BASE-T標準）為了最大程度的減少衝突，最大程度的提高網路速度和使用效率，使用交換機（Switch）來進行網路連接和組織，這樣，乙太網路的拓撲結構就成了星型，但在邏輯上，乙太網路仍然使用匯流排型拓撲和CSMA/CD（Carrier Sense Multiple Access/Collision Detect即帶衝突檢測的載波監聽多路訪問）的匯流排爭用技術。

典型的OSI模型的七層架構



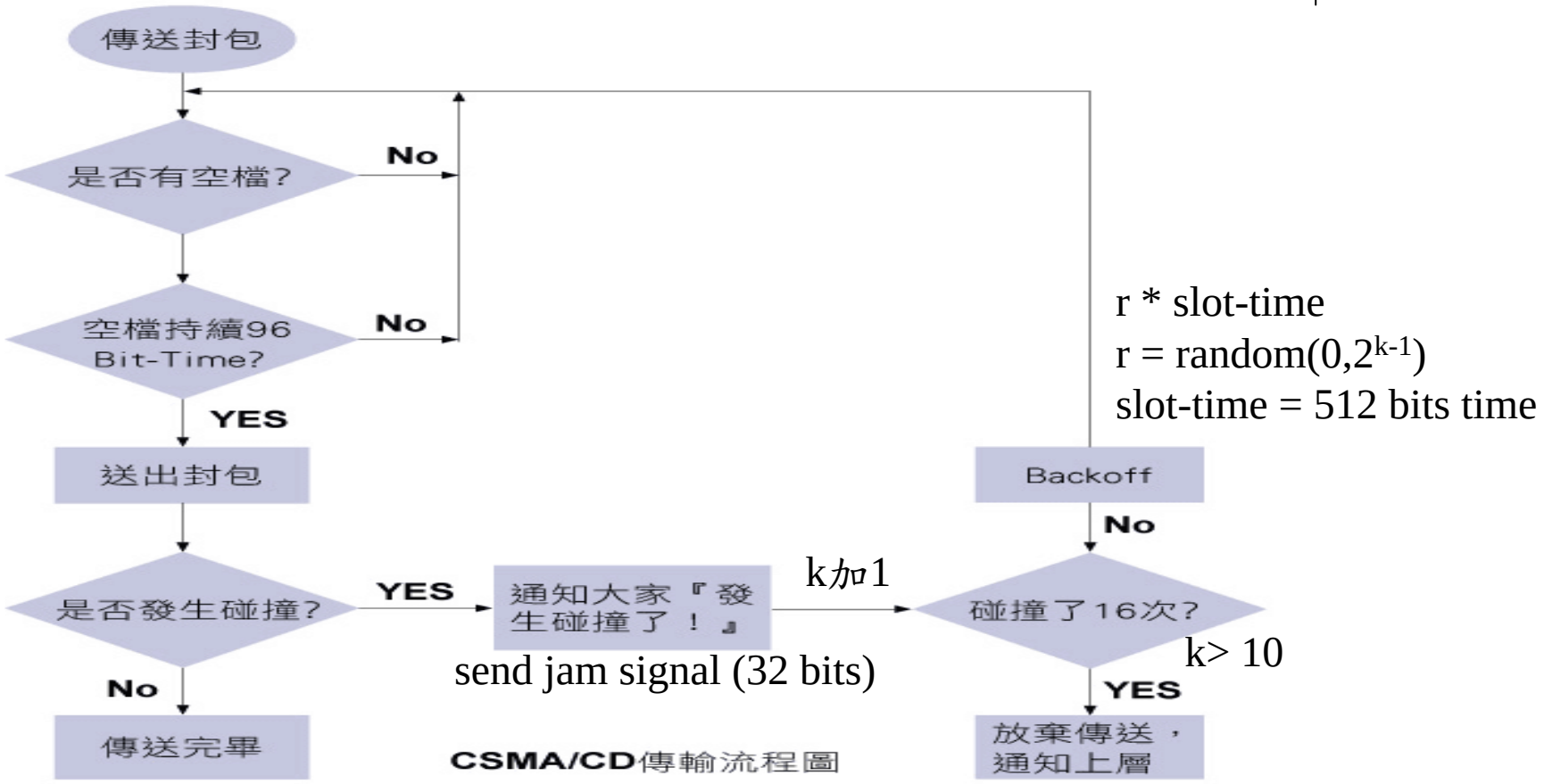
通訊傳輸功能上的資料處理單位、通訊位置和裝置名稱

OSI分層	資料處理單位	通訊位置	裝置名稱
Transport （傳輸層）	Segment （區段）	Host-to-Host （End-to-End） （主機對主機）	Gateway （閘道器）
Network （網路層	Packet （封包）	LAN-to-LAN （區域網路對區域網路）	Router （路由器）
Data link （資料鏈結層）	Frame （框架）	Devices or LAN （一群裝置或區域網路）	Bridger （橋接器）
Physical （實體層）	Bit or Byte （位元或位元組）	Device-to-Device （point-to-point） （裝置對裝置）	Repeater （訊號放大器）

CSMA/CD原理

- 在網路上任何一台工作站主機要與網路上任何一台工作站或伺服器從事資料傳輸時，該主機要先傾聽（listen）網路上是否有其它工作站也在發出要求傳送資料到網路的信號，如果剛好兩台工作站主機一起同時發出信號，結果勢必產生信號碰撞，此時兩台工作站同時退出上網路爭奪戰，等一段任意時間（random time）後再重新發出上網路信號，如果很慶幸這個時段網路上沒有任何其他信號存在後，該工作站就可以傳輸資料至其欲送達之目的地，如果很不幸又發生碰撞或是網路還在從事資料傳輸工作，碰撞事件免不了要發生，因此該工作站仍須等一段任意時間後再嘗試下次機會，這種運作方式稱之為CSMA/CD

CSMA/CD的傳送流程

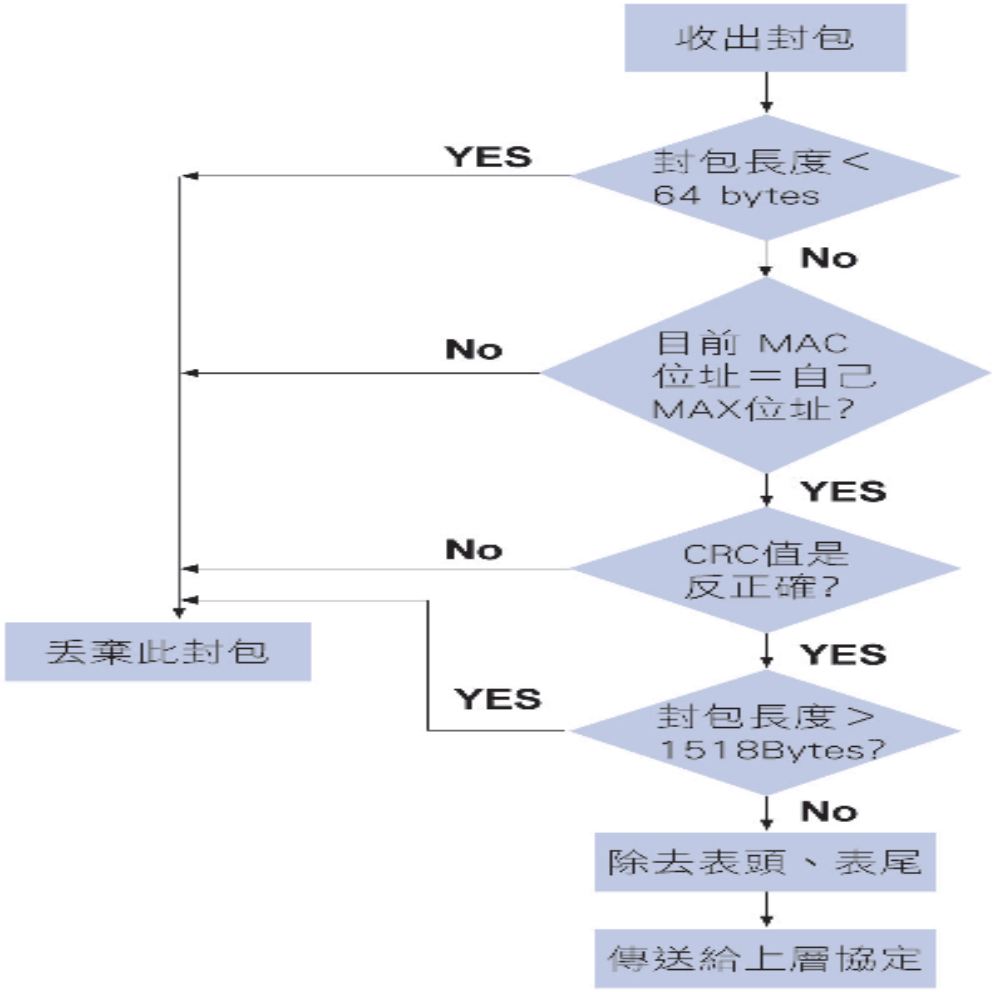


r * slot-time
r = random(0,2^{k-1})
slot-time = 512 bits time

乙太網路採用「廣播」（Broadcast）方式傳送框架

- 框架一旦傳送出去，網路上的所有電腦，無論是否為傳送對象，都會收到此框架。
- 為了使每一部電腦都能知道自己是否為傳送的對象？因此每張Ethernet網路卡都編有一個獨一無二的MAC（Media Access Control）位址，也有人將MAC 址稱為硬體位址（Hardware address）、Physical address或Layer 2 address。
- 由於每個框架都會記載「來源MAC位元址」和「目的MAC位元址」。所以每台電腦在比對目的MAC位元址之後，就可以得知自己是否為傳送的對象。若非傳送的對象，便丟棄此框架；若是傳送的對象，便繼續處理此框架。

CSMA/CD的接收流程



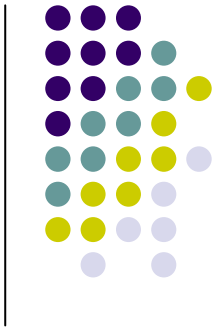
乙太網路四個重大缺失

1. 由於採競爭式所以無法保證時效，所以需要時效多媒體的通訊並不可使用，或許讀者會說我還是可以在網路上聽廣播、打Skype等，請注意乙太網路可是在1975年就有了，目前雖然因通訊電子技術進步和頻寬增大，好像可以滿足時效性要求，但是不像電信網路系統般一定可以保證時效。
2. 安全性有疑慮，因為要先傾聽網路上是否有其他工作站也在發出要求傳送資料到網路的信號，所以當乙太網路進入雜亂（promiscuous）模式時會將所有框架接收，這時他人便可以窺視（sniffer）你的通訊內容，日後我們用Wireshark協定分析實驗也就是用此模式。

乙太網路四個重大缺失

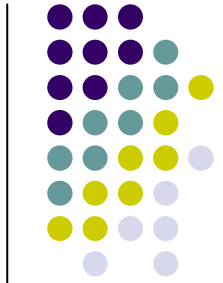
3. 不確定目的端是否有接收到，CSMA/CD傳送採非連接導向式（connectionless）方式通訊，所以發送端根本不知接收端是否有正確接收到框架。
4. 由於採競爭式系統故效率差，況且無法排除碰撞，當產生碰撞後等一段時間依舊會進入系統中競爭，容易有滾雪球效應而讓系統進入擁塞（congestion）後崩潰。

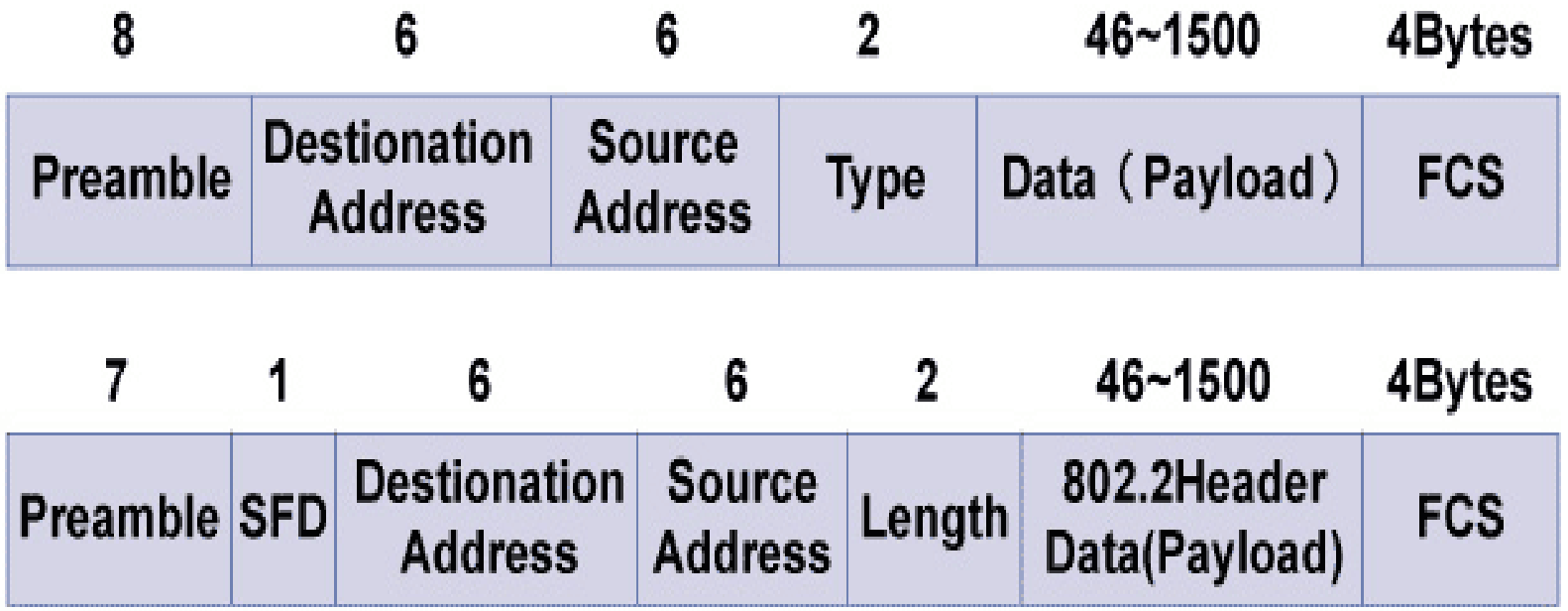
乙太網路框架格式



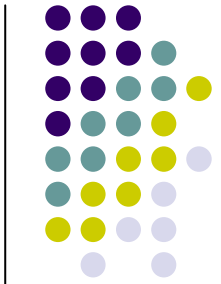
- 現行對乙太網路標準的訂定常用的大致有兩個，一個是以DEC（迪吉多電腦）、INTEL（英特爾）與Xerox（全錄）三家公司所共同制定的DIX乙太網路標準，目前常見的是Ethernet II，又稱作EV2框架
- 另一個則是由IEEE802委員會所制定的IEEE802.3標準。
- 至於網路系統中要如何決定採用何種框架格式，並非由使用者決定，而是要配合上層協定和下層網路卡驅動程式，這兩者都和作業系統關係密切，一般而言以Ethernet II為主，僅有少數系統使用802.3格式的框架，如IPX和Cisco Spanning Tree等。

乙太網路框架格式




8
6
6
2
46~1500
4Bytes
Preamble
Destionation Address
Source Address
Type
Data（Payload）
FCS
7
1
6
6
2
46~1500
4Bytes
Preamble
SFD
Destionation Address
Source Address
Length
802.2Header Data(Payload)
FCS

乙太網路框架格式



- Preamble（前序）：佔8 Bytes，前七個Bytes用以提供執行系統訊號同步處理工作，第八個Byte代表Preamble與框架內容的分界；也就是說，從這個BYTE之後的資料才會被網路設備視為框架內容開始解讀。在IEEE802.3將第八個Byte獨立出來，稱之為SFD（Start Frame Delimiter；起始框訊分界元）欄位，其實其整體的內容與功用與Ethernet2.0是一樣的。

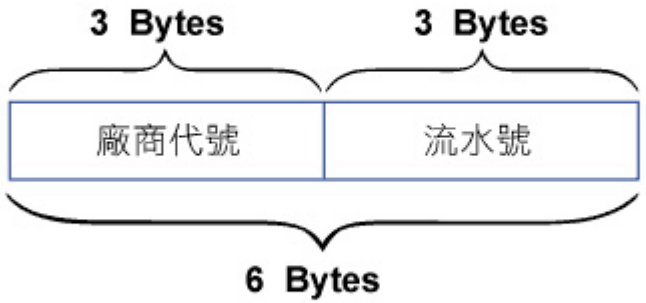
(一般提到的乙太網路框架長度都沒有包含Preamble的長度。)

乙太網路框架格式

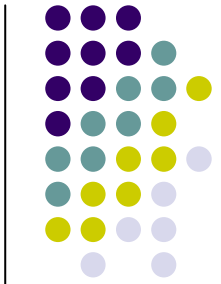
- Destination MAC Address（目的MAC位元位址）：佔六個Bytes，紀錄此框架的目的MAC位址。其前3 Bytes為廠商代號，後3 Bytes則是網路卡序號。當所有MAC位址位元均為1時，也就是連續48個位元均為1的MAC位址（表示為FF-FF-FF-FF-FF-FF），代表提供進行廣播使用的廣播位址（Broadcast Address），通常在不知目的端實體位元址的情況下，即以這個位址進行網路的通訊工作。

乙太網路框架格式

- Source MAC Address（來源MAC位址）：佔六個Bytes，紀錄此框架的來源MAC位址。值得注意的是，此欄位必定是指某個特定的AC位址，不可能是廣播位址。



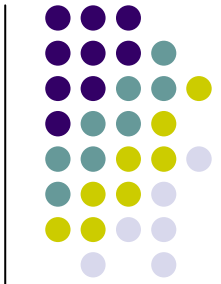
乙太網路框架格式



- Type（協定種類）：佔兩個Bytes，以代碼指定上層（網路層）所採用的協定；由於屬於網路層的協定相當多，因此在乙太網路標頭中，便藉助這個欄位對上層協定形態做定義，不同的協定有不同的辨識碼，例如0600代表XNS、0800代表IP、8137代表IPX等等。因為網路層可能同時安裝TCP/IP、IPX、NetBeui等多種協定，此欄位便指出應將Payload傳給上層的哪一種協定處理。

(在IEEE802.3中，將TYPE欄位改為LENGTH記載長度。)

乙太網路框架格式



- Data（資料）：這是用以放置資料訊息的位置，資料欄位的總長度必須在46~1500位元組之間，不足46個位元組時，必須在此欄位填入任意位元組（一般為00）進行填充，超過1500位元組的資料，則必須使用另一個框架傳送。
- 在IEEE802.3規格挪用了Payload的前三個Bytes，這三個Bytes的用途定義在802.2規格中，分別是DSAP（Destination Service Access Point；目的端服務存取點）、SSAP（Source Service Access Point；來源端服務存取點）及CTRL控制欄位元，而網路層協定便透過服務存取點來進行資料轉送處理溝通的工作。

乙太網路框架格式

- FCS（Frame Check Sequence框架檢查序列）：佔四個Bytes，用來檢查訊框內資料位元是否正確，欄位數值採用CRC方式運算出來。即記錄著由硬體（網路卡）自動產生的CRC值，將來接收端收到框架時，也會產生一個CRC值，並比對兩個CRC值是否相符，以判斷框架是否完整無損。

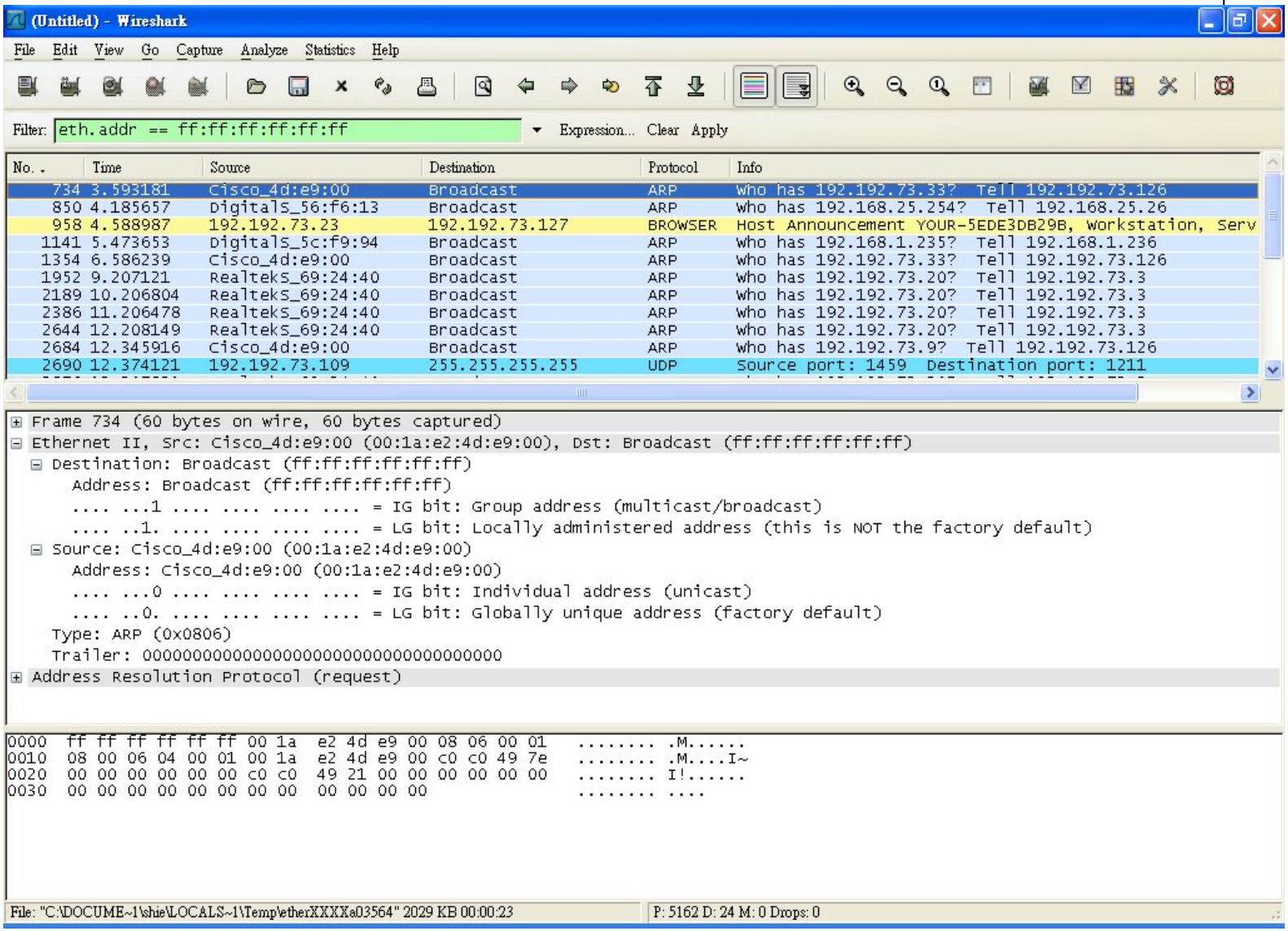
分辨Ethernet II封包與IEEE802.3封包

- 在同樣位置的內容，802.3視為「長度」，而Ethernet II視為「代碼」。802.3長度的最大值為1500，而Ethernet II的最小代碼為0600（相當十進位的1536），所以從數字大小就能判斷出來。
- 若想瞭解電腦網路卡的MAC位址，可以運用ipconfig/all指令進行。

實驗方法

- Ethereal（or Wireshark）為目前使用最廣的網路協定分析工具，版權是屬於免費開放原始碼的軟體（GNU General Public License version 2），通常用於網路通訊協定分析、故障排除、監聽異常封包及問題封包檢測等的教育訓練。最早名稱是Ethereal，但其主要開發人員Gerald Combs從NIS跳槽到CACE，所以該計畫的名稱改為Wireshark。
- 使用Ethereal(or Wireshark)如果能適當設定過濾器(filter)可讓封包解析的工作方便些，例如只要解析通訊協定Type為IP的框架資料可以設定過濾器：「eth.type==0x800」，要解析目的地IP位此為192.192.73.46的telnet封包可以設定過濾器：「ip.dst == 192.192.73.46 AND tcp.port == 23 AND eth.type == 0x800」。

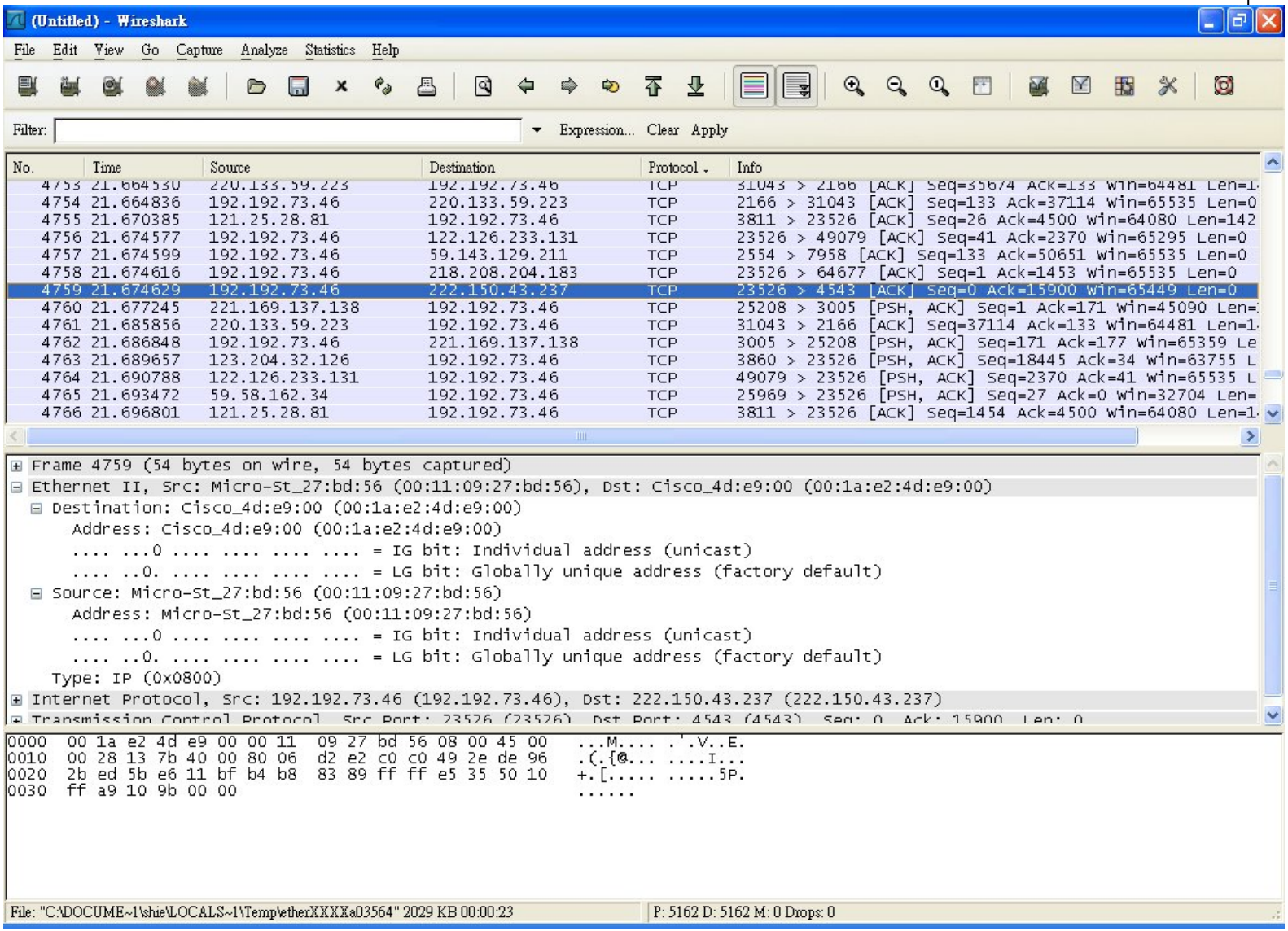
Ethernet II框架



Ethernet II框架

- Destination（目的位址）：ff:ff:ff:ff:ff:ff，廣播位置。
- Source（來源位址）：00:1a:e2:4d:e9:00，（00:1a:e2表示為Cisco）。
- Type（協定種類）：0x0806，所以為ARP。
- Trailer（拖尾）：由於ARP協定內容僅有28位元組不足46位元組，補充18位元組。

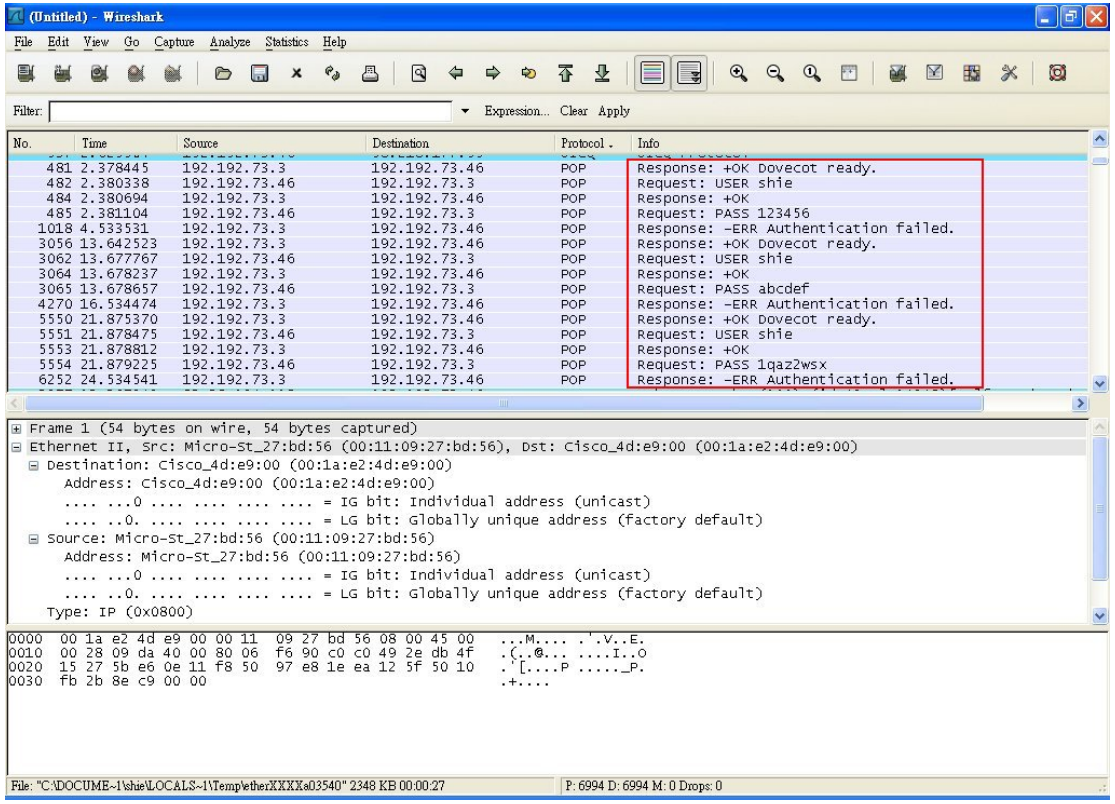
Ethernet II框架



Ethernet II框架

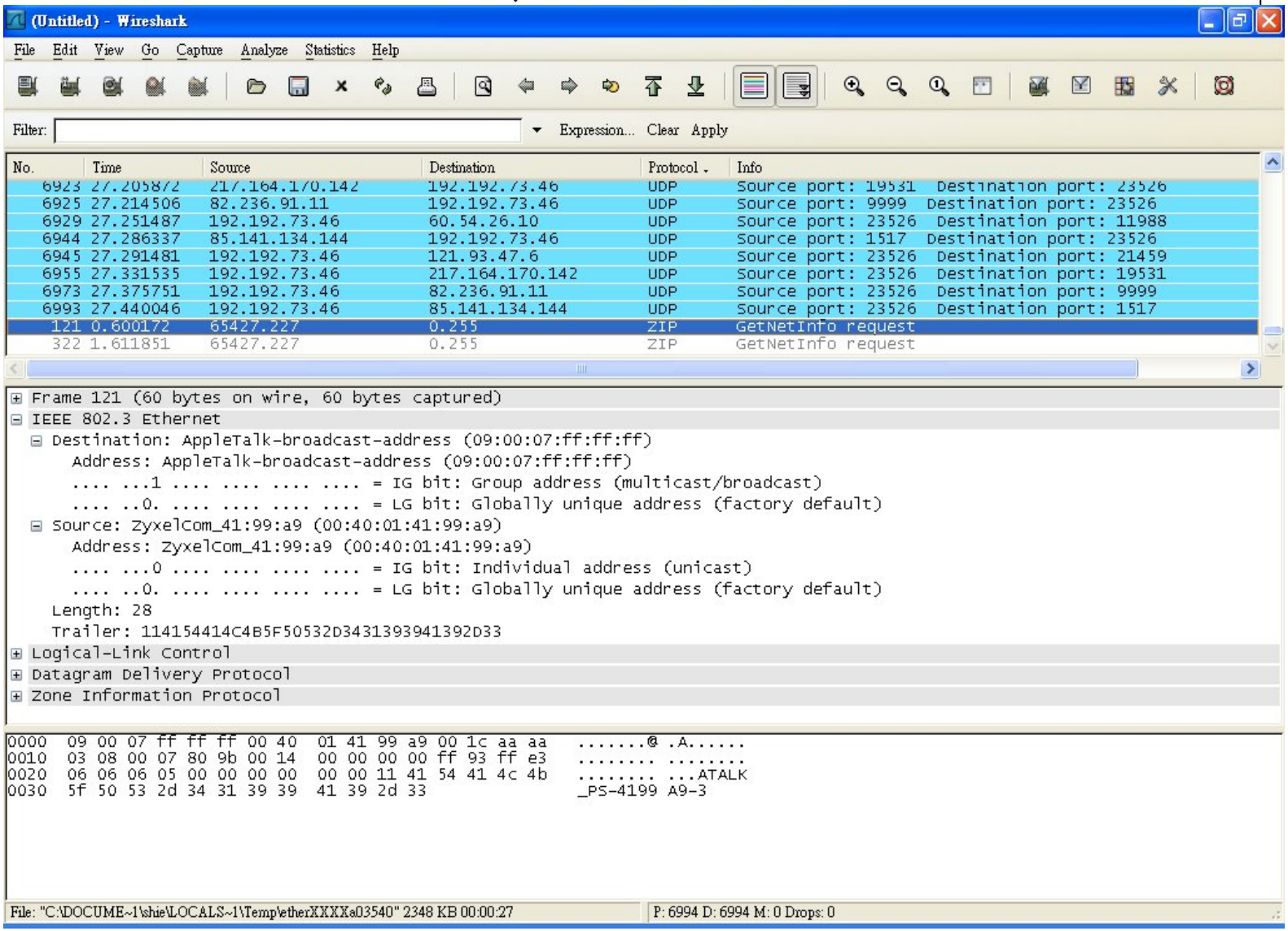
- Destination（目的位址）：00:1a:e2:4d:e9:00，（00:1a:e2表示為Cisco）。
- Source（來源位址）：00:11:09:27:bd:56，（00:11:09表示為Micro-St）。
- Type（協定種類）：0x0800，所以為IP。

Ethernet II框架



可以看到POP協定的密碼，這也就是許多公司不許員工使用Outlook（express）收發信的原因。

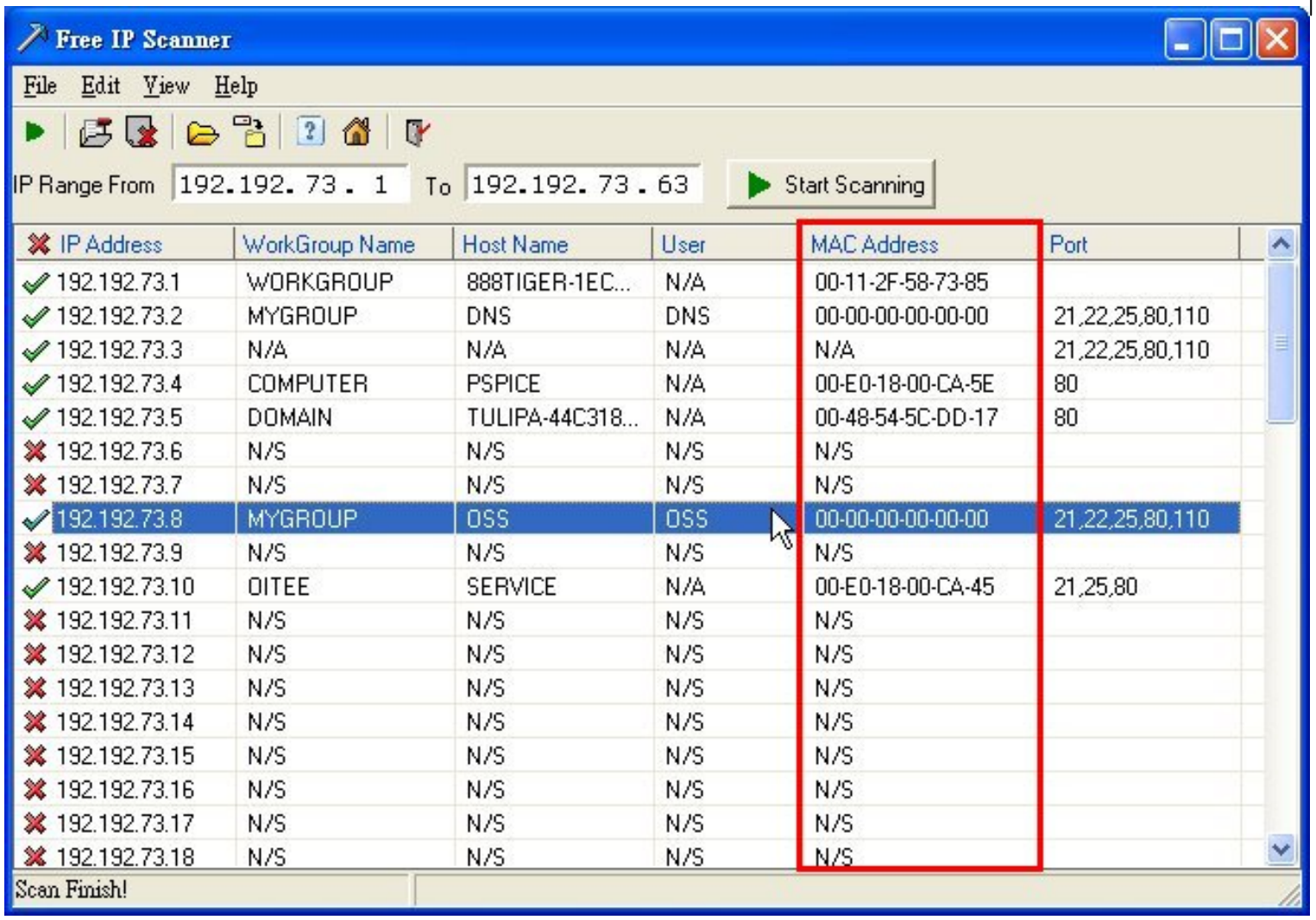
IEEE 802.3框架


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
6923 27.205872 217.164.170.142 192.192.73.46 UDP Source port: 19531 Destination port: 23526
6925 27.214506 82.236.91.11 192.192.73.46 UDP Source port: 9999 Destination port: 23526
6929 27.251487 192.192.73.46 60.54.26.10 UDP Source port: 23526 Destination port: 11988
6944 27.286337 85.141.134.144 192.192.73.46 UDP Source port: 1517 Destination port: 23526
6945 27.291481 192.192.73.46 121.93.47.6 UDP Source port: 23526 Destination port: 21459
6955 27.331535 192.192.73.46 217.164.170.142 UDP Source port: 23526 Destination port: 19531
6973 27.375751 192.192.73.46 82.236.91.11 UDP Source port: 23526 Destination port: 9999
6993 27.440046 192.192.73.46 85.141.134.144 UDP Source port: 23526 Destination port: 1517
121 0.600172 65427.227 0.255 ZIP GetNetInfo request
322 1.611851 65427.227 0.255 ZIP GetNetInfo request
Frame 121 (60 bytes on wire, 60 bytes captured)
IEEE 802.3 Ethernet
Destination: AppleTalk-broadcast-address (09:00:07:ff:ff:ff)
Address: AppleTalk-broadcast-address (09:00:07:ff:ff:ff)
....1 .... = IG bit: Group address (multicast/broadcast)
.... ..0. .... = LG bit: Globally unique address (factory default)
Source: ZyxelCom_41:99:a9 (00:40:01:41:99:a9)
Address: ZyxelCom_41:99:a9 (00:40:01:41:99:a9)
....0 .... = IG bit: Individual address (unicast)
.... ..0. .... = LG bit: Globally unique address (factory default)
Length: 28
Trailer: 114154414C4B5F50532D3431393941392D33
Logical-Link Control
Datagram Delivery Protocol
Zone Information Protocol
0000 09 00 07 ff ff ff 00 40 01 41 99 a9 00 1c aa aa ....@ .A......
0010 03 08 00 07 80 9b 00 14 00 00 00 00 ff 93 ff e3 ....
0020 06 06 06 05 00 00 00 00 00 00 11 41 54 41 4c 4b ....ATALK
0030 5f 50 53 2d 34 31 39 39 41 39 2d 33 _PS-4199 A9-3
File: "C:\DOCUME~1\shie\LOCALS~1\Temp\etherXXXXa03540" 2348 KB 00:00:27
P: 6994 D: 6994 M: 0 Drops: 0

IEEE 802.3框架

- Destination（目的位址）：09:00:07:ff:ff:ff，（09:00:07表示為Apple-Talk）。
- Source（來源位址）：00:40:01:41:99:a9，（00:40:01表示為Zyxel-Com）。
- Length（長度）：28。
- Trailer（拖尾）：由於ZIP協定內容僅有28位元組不足46位元組，補充18位元組。

使用Free IP scanner來檢視區域網路上所有的IP/MAC對。



本章註解

1. OSI模型的七層架構僅是具參考而已，並沒有真正實施過，可參考本書實驗11。
2. Ether是物理上美麗的錯誤，原指在宇宙中到處都有的物質用來載送光波，Ethernet原義也是希望該網路架構可以充斥宇宙的每一個角落。
3. IEEE 802.3可參考http://www.ieee802.org。
4. 讀者可參考ALOHA、slotted ALOHA、CSMA 、CSMA/CD與CSMA/CA的演進史。
5. 「廣播」在此是指只要功率可及而不管目的地，這可是電信網路和計算機網路最大的差別。
6. 所有Ethernet網路卡的廠商都必須向IEEE註冊，以取得廠商代號，此代號稱為OUI（Organizationally Unique Identifier），原本是獨一無二的，但不要太相信它，可參考本書實驗11。
7. 學習協定的自我評定指標之一是看能否能瞭ipconfig/all中所有數目背後的意義。

學習評量

1. 說明OSI模型的7層架構沒有普及的原因？
2. 為何乙太網路不適合高負載及即時應用環境？
3. 乙太網路是如何來判斷網路是否有發生碰撞？
4. 何謂「二元指數後退演算法」（Binary Exponential Backoff Algorithm）？
5. 在乙太網路中，為何需要最小訊框限制？它的最小訊框是多少？如果訊息長度不及的情況下，應如何克服？
6. 使用乙太網路的風險何在？
7. 乙太網路的效能如何評估？
8. 乙太網路為何能在Token Ring、Token bus等不同區域網路協定中勝出？
9. Ethernet、Fast Ethernet與Giga bit Ethernet的演化過程如何？
10. 協定解析軟體還有哪些？