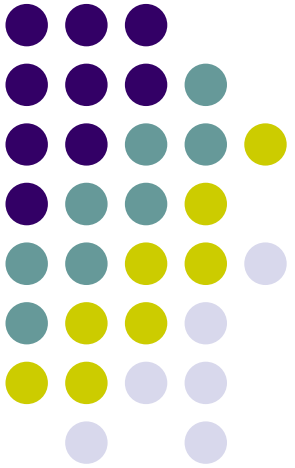
# 實驗3 IP協定分析

**實驗目的**

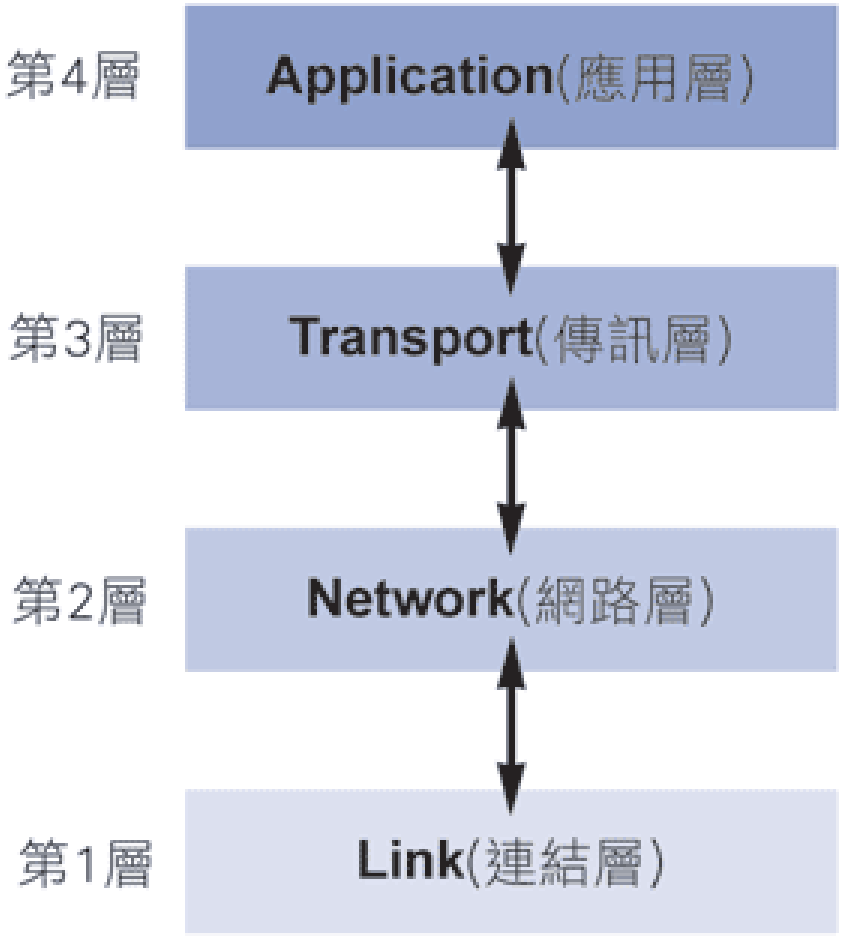
- 明瞭IP（Internet Protocol；Internet協定）的基礎觀念
- 解析IP協定下，IP封包格式、IP封包傳送、IP封包切割與重組



# 背景資料

- IP位於DoD模型的網路層（Network Layer），對上可載送傳輸層（Transport Layer）各種協定的資訊，例如：TCP、UDP等等；對下可將IP封包放到資料連結層（Data Link Layer），透過乙太網路、Token Ring、FDDI等規格的技術來傳送。

# 網際網路協定模型


第4層
Application(應用層)
第3層
Transport(傳訊層)
第2層
Network(網路層)
第1層
Link(連結層)

# 網際網路技術發展

- 網際網路是美國防衛司令部（相當我國的國防部）為了防止核攻擊而產生的資料傳遞技術。
- IP的技術觀念核心就是Best-effort，意思即是盡它最大的努力但是不保證送到。
- IP是採用非連接導向式（connectionless）的傳輸，並且隱含著具有自癒能力，也就是說當封包自發送端出發後，它所經過的路徑可能依網路的情況加以變化，發送端並無法確定封包是否正確到達目的端，更不保證封包到達的順序。
- 可以將IP技術視為郵政系統，民眾將信件投入郵筒中，並不知道郵差何時將你的郵件遞送給收信者也不知道收信者是否真能收到該郵件，當然郵政系統也會努力盡責地盡快傳送郵件，但有時也會因為一些因素，如天候、交通、戰爭等使得郵件無法遞送。

# 網際網路技術發展

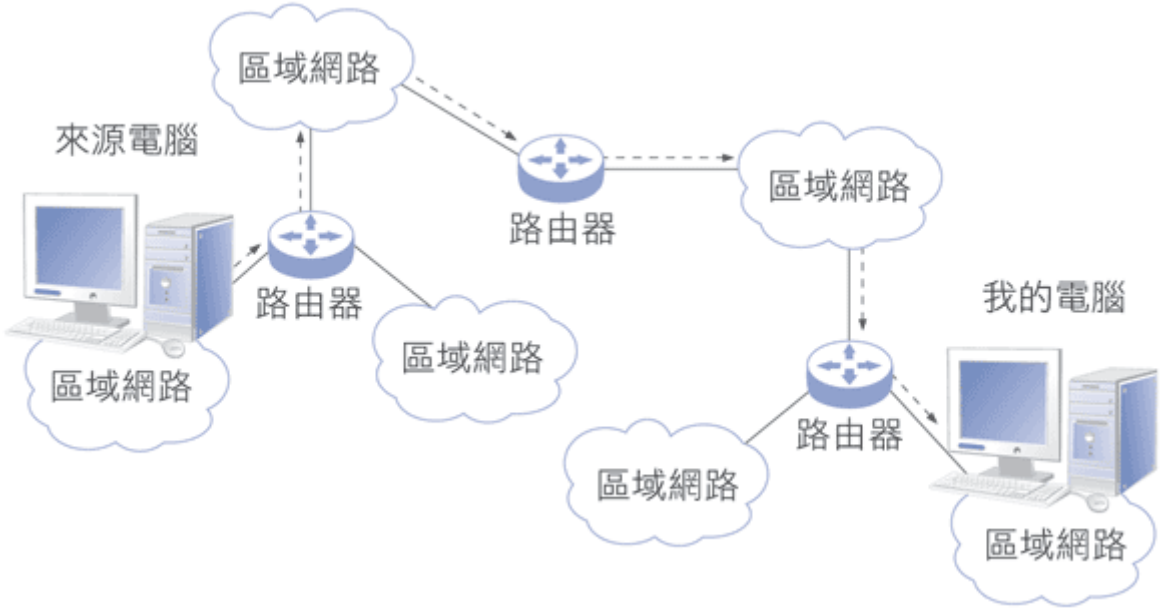
- IP是整個網際網路協定的重要基礎，其功能如下：
  - 定義網際網路中傳輸的基本單位。
  - 定義網際網路的定址方式。
  - 負責網路存取層和傳送層之間的資料傳遞。
  - 決定資料傳送的路由路徑。
- 基本上IP所提供的服務有封包傳送、封包的切割與重組兩種。

# IP封包的傳送

- IP負責將封包從來源裝置傳送到目的裝置。為了能夠正確的指出目的裝置的位置，因此IP規定所有使用IP的裝置，都必須有一個獨一無二的IP位址（類似現實世界中郵政系統的地址）以供區分辨別，同時方便傳送IP的封包。
- 網際網路中是由許多個網路相互連結而成，因此必須透過IP路由（IP Routing，類似現實世界中郵政系統的郵局角色）的轉送，才能將IP封包經過一個個的網路送達目的地。

# IP封包的傳送

- 每個網路是透過路由器（Router）來相互連接。換言之，IP封包必須靠沿途各路由器的通力合作，才能到達目的地。



# IP封包的切割與重組

- 由於每一種資料連結層都有所謂的MTU（Maximum Transmission Unit；最大傳輸單位），因此路由器必須有IP封包的切割與重組機制，即是將過長的封包加以切割，以便能在MTU較小的網路上傳輸。
- 切割後的IP封包，會由目的裝置重組，恢復成原來IP封包的模樣。

# IP封包的切割與重組

- 列舉幾種常見技術的MTU：

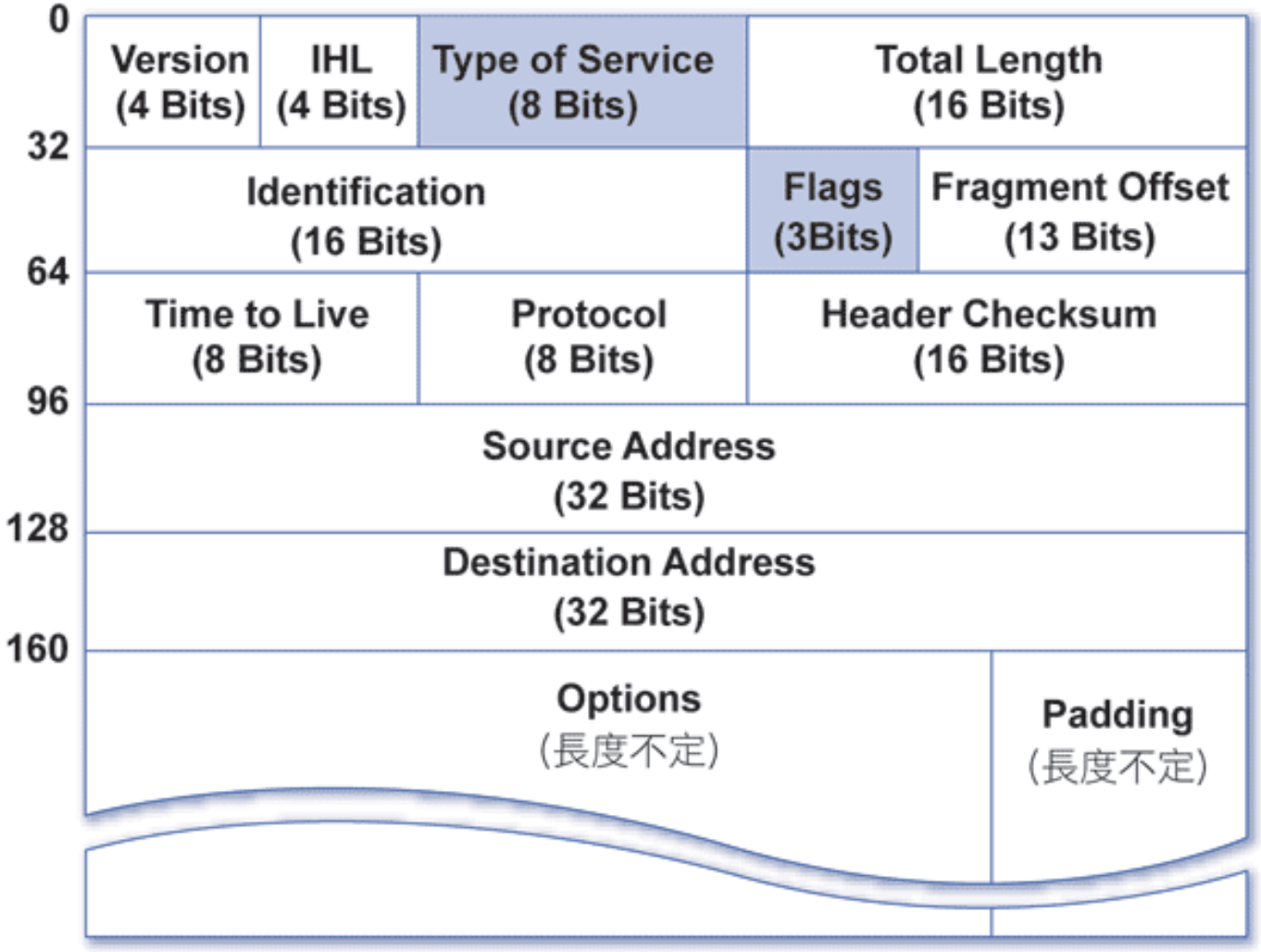
| 技術 | MTU |
| --- | --- |
| 乙太網路 | 1500 Bytes |
| FDDI | 4352 Bytes |
| X.25 | 1600 Bytes |
| ATM | 9180 Bytes |

# IP封包資料

- IP封包資料包括IP表頭和資料，然後往下在資料鏈結層中被資料鏈結層表頭和資料鏈結層表尾包圍，如下圖：


- IP表頭：記錄有關IP位址、路由、封包識別等資訊。長度為4 Bytes的倍數，最短為20 Bytes，最長可達60 Bytes。
- IP Payload（使用者資料）：載送上層協定的封包。長度最短為8 Bytes，最長可達65515 Bytes。

# IP表頭欄位定義


0
32
64
96
128
160
Version (4 Bits)
IHL (4 Bits)
Type of Service (8 Bits)
Total Length (16 Bits)
Identification (16 Bits)
Flags (3Bits)
Fragment Offset (13 Bits)
Time to Live (8 Bits)
Protocol (8 Bits)
Header Checksum (16 Bits)
Source Address (32 Bits)
Destination Address (32 Bits)
Options (長度不定)
Padding (長度不定)

# IP表頭欄位定義

- Version（版本號碼）：佔4 Bits，記錄IP的版本編號。目前最常見的IP版本為第四版的IP規格，欄位值為4（0100二進位）；若採用第六版IP規格，這個欄位的值便會是6（0110）。
- IHL（Internet Header Length；表頭長度）：佔4 Bits，記載此IP表頭的長度，而且表頭長度的計算是以4 Bytes為基本單位；例如：IHL欄位值為0101（二進位），即代表IP表頭的長度為5 x 4 = 20 Bytes，最長可達15x 4 = 60 Bytes。

# IP表頭欄位定義

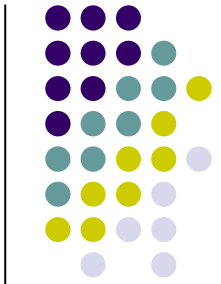
- Type of Service（服務類型）：佔8 Bits，包含了六個參數。
  - 第一個參數Precedence佔3 Bits，是用來決定IP封包的優先等級，參數值愈大代表優先等級愈高，各參數值的意義如下表：

| 參數值（二進位） | 參數值（十進位） | 說明 |
|---|---|---|
| 111 | 7 | Network Control |
| 110 | 6 | Internetwork Control |
| 101 | 5 | CRITIC／ECP |
| 100 | 4 | Flash Override |
| 011 | 3 | Flash |
| 010 | 2 | Immediate |
| 001 | 1 | Priority |
| 000 | 0 | Routine |

# IP表頭欄位定義

- 第二個參數Delay（延遲性）佔1 Bit，用來定義IP封包對於延遲性的要求，0代表一般延遲，1代表低延遲，如語音訊號的傳輸便必須採用低延遲的傳送型態。
- 第三個參數Throughput（傳輸量）佔1 Bit，用來定義IP封包對於頻寬的要求，0代表一般傳輸量，1代表高傳送量，如大檔案的資料傳送時常將此位元設為1。
- 第四個參數Reliability（可靠度）佔1 Bit，用來定義IP封包對於路徑可靠度的要求，0代表低可靠度，1代表高可靠度，如應用程式希望在傳送過程中盡量減少IP封包的遺失，則可設為高可靠度的傳輸。
- 第五個參數Cost（成本）佔1 Bit，用來定義IP封包對於路徑成本的要求，0代表低成本，1代表高成本，一般預設為0。
- 第六個參數Reserved保留未使用。

# IP表頭欄位定義



- Total Length（封包總長度）：佔16 Bits，記錄整個封包的長度，包含IP表頭及IP所帶資料內容的總和，單位為Byte；以乙太網路為例，整個IP封包最大可達1500 Bytes，所以此欄位的最大值即為1500（十進位）。
- Identification（識別碼）：佔16 Bits，記錄IP封包的識別碼。由發送端對每一個IP封包進行唯一辨識代碼的設定，以便接收端可以根據此辨識碼執行封包辨識工作，若封包在傳輸過程中因為MTU（最大傳輸單位）的限制，導致傳輸過程中，將封包切割成幾個Fragments（片段）進行傳送，而因為每個IP封包到達目的裝置的先後順序可能與出發時的順序不同，因此接收端在進行封包重組時，便必須以此識別碼進行判斷IP封包原來的順序，以便能將屬於相同資料封包的片段組合在一起。

# IP表頭欄位定義

- Flag（封包切割旗標）：佔3 Bits，主要對IP封包的切割提供控制訊息。第一個位元未定義，設定為0；第二個位元DF定義封包是否可加以切割，0代表可切割，1代表不可切割；第三個位元MF，定義此傳輸封包是否為原始封包的最後片段，0代表最後片段，1代表尚有其他片段。

| 位置 | 參數名稱 |
| --- | --- |
| 第1Bit | 保留 |
| 第2Bit | DF（Don’t Fragment） |
| 第3Bit | MF（More Fragments） |

# IP表頭欄位定義

- Fragment Offset（片段位移）：佔13 Bits，用來記錄IP Fragment所載送的是原始IP Payload的哪一段資料。因IP封包切割後，原始封包內IP Payload的資料會分散到每個IP Fragment中，因此需要分別註明以便重組。Fragment Offset的單位是8 Bytes。
- 以乙太網路的封包切割為例，如果原來在網路系統中有4500 Bytes資料需要進行傳送，若IP表頭有20 Bytes，因此真正的資料長度為4480 Bytes，由於乙太網路的MTU只有1500 Bytes，因此封包的傳輸就必須切分成幾個片段，片段仍然需要提供20個位元組給IP表頭使用，因此，一個乙太網路訊框真正可以傳輸的資料長度變為1480 Bytes，而其片段位移值的設定，對第一個片段而言，其片段位移值為0，第二個片段的位移值為185（1480/8），第三個片段位移值變為370，而最後一個片段位移值則為555。

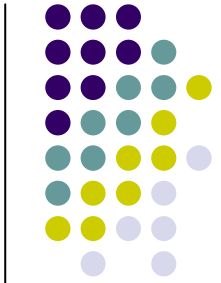
# IP表頭欄位定義


IP表頭
4480Bytes 資料訊框
IP表頭
1480Bytes 資料訊框
FO=0
+
IP表頭
1480Bytes 資料訊框
FO=185
+
IP表頭
1480Bytes 資料訊框
FO=370
+
IP表頭
40Bytes 資料
FO=555

# IP表頭欄位定義

- Time To Live（存活時間）：佔8 Bits，記錄IP封包的「存活時間」，以限制IP封包在路由器之間轉送的次數。當IP封包每經過一部路由器時，路由器便會將Time to Live欄位值減1，當路由器收到此欄位值為1的IP封包時，便直接將之丟棄，不再轉送。
- Protocol（協定）：佔8 Bits，記錄封包在傳輸層所使用的網路協定為何。

# IP表頭欄位定義



- 列舉數種常見的設定值：

| 設定值 | Protocol |
|---|---|
| 1 | ICMP Internet Control Message |
| 2 | IGMP Internet Group Messagement |
| 6 | TCP Transmission Control |
| 17 | UDP User Datagram |
| 50 | ESP Encap Security Payload for Ipv6 |
| 51 | AH Authentication Header for Ipv6 |
| 115 | L2TP Layer Two Tunneling Protocol |

# IP表頭欄位定義

- Header Checksum（表頭檢查碼）：佔16 Bits，用以檢查表頭內容的傳送是否正確，介於來源端與目的端之間的所有路徑器，都會對此欄位執行運算檢查的工作，當檢查均正確無誤時，資料封包才可以順利的抵達目的端。檢查碼運算只針對IP表頭進行檢查，並不會檢查IP Payload的正確性。欄位的初始值運算由來源端負責，運算時將檢查碼欄位值設為0，再將IP表頭內容以16個位元為單位運用1補數演算法進行加總，所得結果再執行1的補數，便為檢查碼的值；接收端或中介節點執行HC欄位檢測時，包含HC值對IP表頭進行加總檢測時，所有位元為1，表示傳輸無誤，否則便需進行偵錯或重傳的工作。

# IP表頭欄位定義

- Source IP Address（來源端IP位址）：佔32 Bits，內容為來源端主機的IP位址。
- Destination IP Address（目的地IP位址）：佔32 Bits，內容為目的端主機的IP位址。
- Options（IP選項）：一般用來網路測試、除錯、安全保密及其他選項，這個欄位為選擇性欄位，並非絕對必要，因此欄位長度不確定。
- Padding（填充）：配合選擇項欄位使用，主要目的在使整個IP表頭的總長度為32位元的整數倍，填補資料以0進行處理。

# IP位址

- 第一階段：Class A、B、C、D、E分類，這是IP在設計最初時，著眼於當時計算機的效能和數量而制定的，結果後來因位址分配不均而產生位址不足的問題。
- 第二階段：子網路遮罩，利用遮罩技術將Class A、B、C、D、E分類法則打破（Classless），產生多個可由網管人員自由分派的子網路。
- 第三階段：網路位址轉換（Network Address Translation；NAT），利用傳輸層的埠號觀念，將多個未註冊的IP位址對應到單一個註冊的 IP位址（多對一）。
- 第四階段：IPv6，第六版IP技術，主要將IP位址擴充至$2^{16*8}$。
- 第五階段：Softether，主要概念是將在網際網路最底層DLC（或對應OSI Level 2 ，即資料連結層）的通訊內容資料框封裝到傳輸層，利用TCP雙向傳輸特性，加上隧道（Tunnel）技術，建構突破地域的超大型虛擬區域網路。

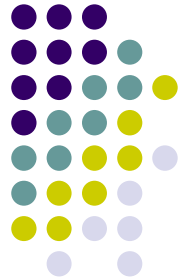
# IP位址

- IPv4位址本是一個長度為32Bits的二進位數值，為一長串的0或1，由於不便為人閱讀，所以8 Bits為單位，將IPv4位址分成四段，將各段的二進位數值轉換成十進位，並以「.」（念dot）隔開。
- 例如11010010110000001101111101101111，我們將它記為210.192.223.111。

# IP位址

- IPv4依據目的裝置的數量不同總共有三種傳遞模式：
  - Unicast：一對一的單點傳遞模式，當來源裝置發出IP封包時，只有該指定的單一目的裝置會收到此IP 封包，在目前網際網路上傳輸的封包，絕大多數都是Unicast的IP封包。
  - Broadcast：一對全部的廣播傳遞模式，在此所指的全部意指所有具有相同網路號的目的裝置。
  - Multicast：一對多的多播傳遞模式，當來源裝置發出IP封包時，可以將封包傳送給一群指定的目的裝置，在目前網際網路上部分網路連線遊戲、網路廣播、P2P傳輸等會使用此模式。

# IP位址



- 由於早期計算機效能的問題，路由器無法採用單一IPv4位址（好比你的手機號碼）來做路由交換（一階段），所以改用折衷的兩階段方式處，將IP位址分為兩個部分所組成，網路位址（Network ID）和主機位址（HostID），路由器僅利用網路位址來做路由交換，等到封包進入目的網路後，再交由目的網路內部自行處理。
- 網路位址：Network ID位於IP位址前端，用來識別所屬的網路，組織或企業申請IP位址時，所分配到的並非個別零散的IP位址，而是取得一個獨一無二的Network ID。
- 主機位址：Host ID位於IP位址後端，用來識別網路上個別裝置，每個裝置的主機位址必須是唯一的。

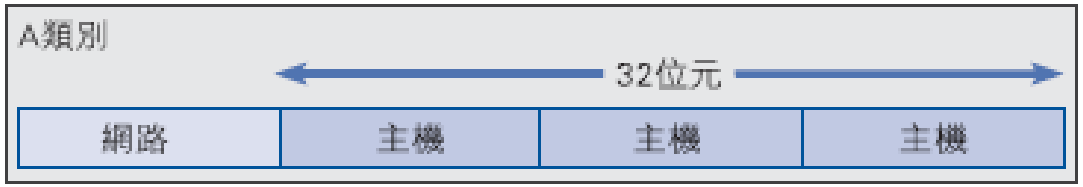
# IP位址

- IP在設計最初時，著眼於當時計算機的效能和數量，制定Class A、B、C、D、E五個分類網路規模，其中Class A、B、C用於Unicast供一般網路裝置使用，Class D用於Multicast，Class E保留為日後發展用。其概念十分淺顯而且易於路由器的處理，當第一個bit為“0”為Class A，路由器取出一個byte做為網路號；當第二個bit為 “0”為Class B，路由器取出二個bytes做為網路號；當第三個bit為“0”為Class C，路由器取出三個bytes做為網路號；當第四個bit為“0”為Class D，路由器做Multicast處理；當第四個bit為“1”則為Class E，目前保留不用。

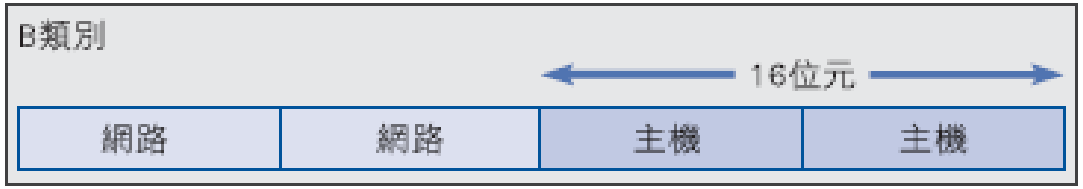
# IP位址

以二進制來看

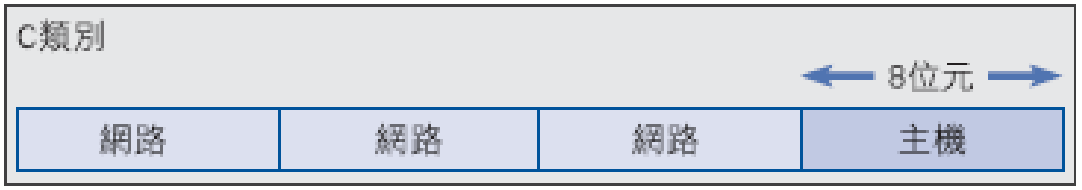
- 如果是以“0”開頭，則是一個A Class的IP。



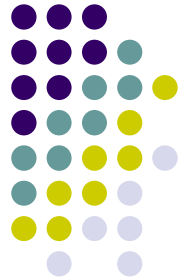

- 如果是以“10”開頭，則是一個B Class的IP。




- 如果是以“110”為開頭，則屬於C Class的IP。



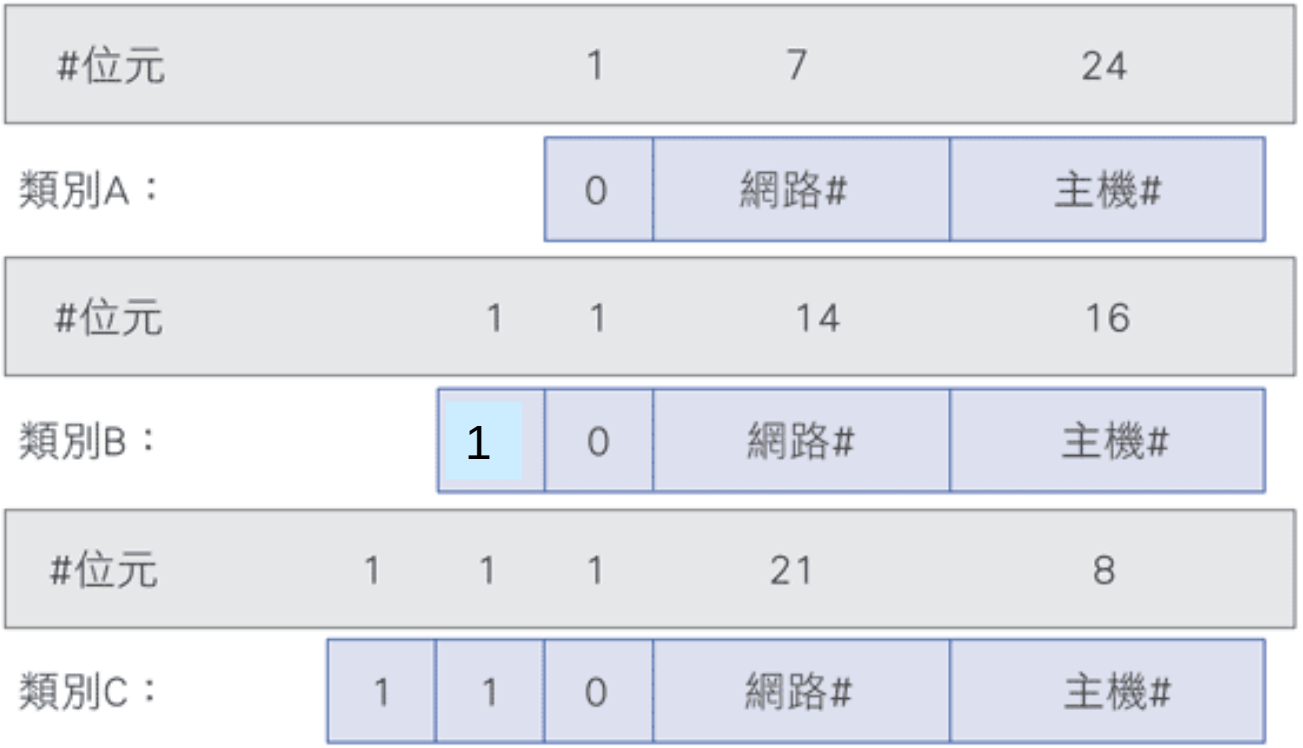
# IP位址



- 以十進制來看
  - 由1到126開頭的IP是A Class。
  - 由128到191開頭的IP是B Class。
  - 由192到223開頭的IP則為C Class。
- 很明顯的，用二進位來判斷IP Class要比用十進制來判斷簡單，當知道如何區分IP的Class之後，就可以知道IP的Net_ID和Host_ID。
  - A Class的IP使用最前面一組數字來做Net ID，剩下三組做Host ID。
  - B Class的IP使用前面兩組數字來做Net ID，另兩組做Host ID。
  - C Class的IP使用前面三組數字來做Net ID，剩下的一組做Host ID。

# IP位址

- 區分三個不同的IP Class：



# 本機迴路（Loopback）

- 保留的Net ID：127（即二進位的01111111）需要特別一提，它是保留給本機迴路（Loopback）測試使用的，主要是做為網路系統中硬體和軟體的責任分界，因為通訊從最上層開始只會下傳到IP的網路層，隨即繞回來，並不會實際連線到DLC層傳遞出去，所以在早期發展的網路系統上，如果連線不符合預期時可以有效釐清到底是硬體或軟體出錯，而今通常該迴路位置是用來代表任何一台主機本身的IP，也就是自己，雖然不能被運用於實際的連線網路上，但是也沒有藉口說因為沒有網路系統所以沒有辦法做網路作業。雖然整段網路Net ID：127都可以使用，但127.0.0.1是最常被使用的IP。

# IP位址

- 一個規則必須遵守，在IP的網路區段中，第一個Host ID（全部為0）為該網路區段的網路號，最後一個Host ID（全部為1）為該網路區段的廣播號，均不可被指派。
- 例如一個Class C 192.192.73的網路區段，192.192.73.0為該網路區段的網路號，192.192.73.255為該網路區段的廣播號，另外，為了安全起見，路由器會將所有主機的廣播255.255.255.255當成一般區域廣播，不會把封包送到區域網路之外。

# IP位址

- 傳統上會以為將網路區分為大、中、小型網路，然後分別使用不同的Class A、B、C，實際情況恐非如此，讓我們仔細分辨一下。很明顯的，A Class網路可以分配的Host ID比C Class多好幾倍，讓我們算算可以劃分的NetID數目和各等級裡面的Host ID數目即可得知。

# IP位址

- 由表可看出Class A、B、C雖然各有224, 216, 28 個主機數目可分配，但若將這麼多部電腦連接在同一個網路中，勢必造成網路效能的低落，因此實際上不可行。所以在此情況下，是會浪費掉許多IP位址的。

| 等級 | 開頭 | 網路數目 | 主機數目 | 使用範圍 | 申請領域 |
|---|---|---|---|---|---|
| A | 0 | 126 | 16,777,214 | 1.x.x.x到126.x.x.x | 國家級 |
| B | 10 | 16,384 | 65,534 | 128.x.x.x到191.x.x.x | 跨國組織 |
| C | 110 | 2,097,152 | 254 | 192.x.x.x到223.x.x.x | 企業組織 |
| D | 1110 | - | - | 224.-到239.- | 多播傳遞 |
| E | 1111 | - | - | 240.-到255.- | 保留範圍 |

# 實體IP與私有IP

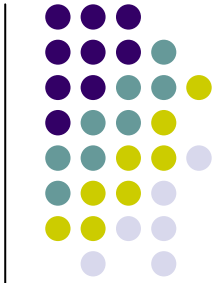
- 當網路連上Internet時，必須先註冊好Net ID，如果該ID已經被使用，就必須使用另外的ID了。負責Internet IP註冊的機構稱之為InterNIC（Network Information Center），其網址是http://www.internic.net，國內的負責單位為TWNIC財團法人台灣網路資訊中心（http://www.twnic.net）。不過，實際上的運作，一般機構或個人是不太可能直接從InterNIC上註冊IP，而是透過ISP來分配，詳細規範可瀏覽TWNIC網站中的「IP/ASN申請」單元。這些經過合法授權使用的IP，稱為實體IP。
- 然而，為了推廣網際網路相關技術且去除網路安全的疑慮，在A、B、C這三個層級裡面，各劃出一些位址範圍保留給私有位址所用，規定這些IP位址不會出現在公眾的網際網路上，這些IP位址被稱為Private（私有）IP位址，所幸有這些保留位址，讓日後NAT技術得以方便些。

# 私有IP位址範圍

| Class | 私有IP位址範圍 |
| --- | --- |
| 1組Calss A | 10.0.0.0 – 10.255.255.255 |
| 16組Calss B | 172.16.0.0 – 172.31.255.255 |
| 256組Calss C | 192.168.0.0 – 192.168.255.255 |

- 使用這些位址時有以下限制：
  - 私有位址的路由資訊不能對外傳播。
  - 使用私有位址做為來源或目的位址的封包，不能透過網際網路來轉送。
  - 關於私有位址的參考記錄，只能限於內部網路使用。

# IPv6



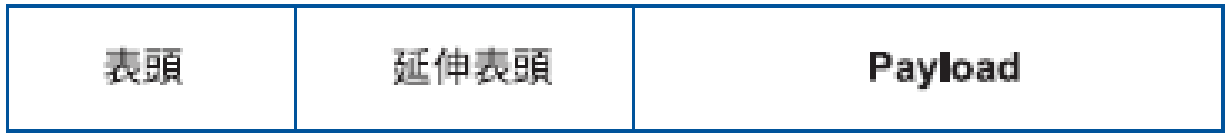
- IPv6於1995年即制定完成，主要的想解決IPv4的種種問題：
  - 提供充足的IP位址數量：IPv6可提供2128 個位址。
  - 頻寬保證：具有Flow Label，加上RSVP協定，可提供項電信服務般的頻寬保證。
  - 安全性：具有加密功能，不怕IP被竊聽竄改。

# IPv6

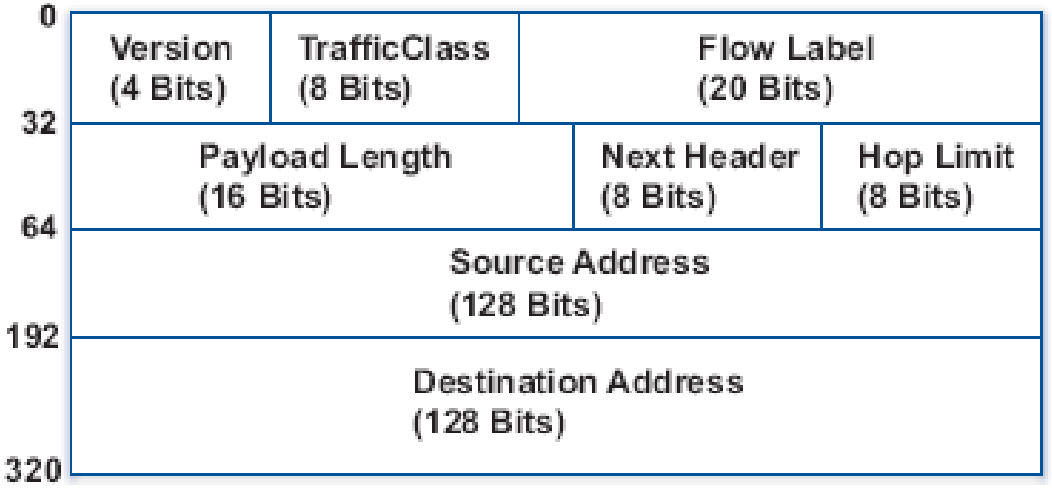
- 看起來是相當完美的解決方案，可是未何遲遲至今尚未普及呢？我們就針對上述三點加以反駁看看：
  - 提供充足的IP位址數量：要提供網路服務者才需實體IP，一般上網使用NAT即可，況且Softether還提供無限大IP位址。還有一個重要因素是美國老大哥IP位址數量當然是充足的，所以目前積極發展IPv6技術的大多是新興國家。
  - 頻寬保證：要做到如電信服務般的頻寬保證，路由器必須全面提昇效能，問題是這筆錢要誰出？管理幾家電信服務公司都很難了，要如何管理為數眾多的網路服務公司呢？
  - 安全性：現有在應用層或IPsec使用加密功能，如果全面提供加密功能，除了增加路由器的負擔外，請問要使用哪一種加密技術呢，大部分加密技術均有專利權的問題，況且美國還將部分加密技術視為軍事武器禁止出口，還有些國家根本禁止人民間的通訊加密。

# IPv6

- 由於目前IPv6尚未普及所以僅提供IPv6 封包的結構與表頭欄位，如果讀者有需要可參考相關書籍。IPv6 封包結構圖如下：

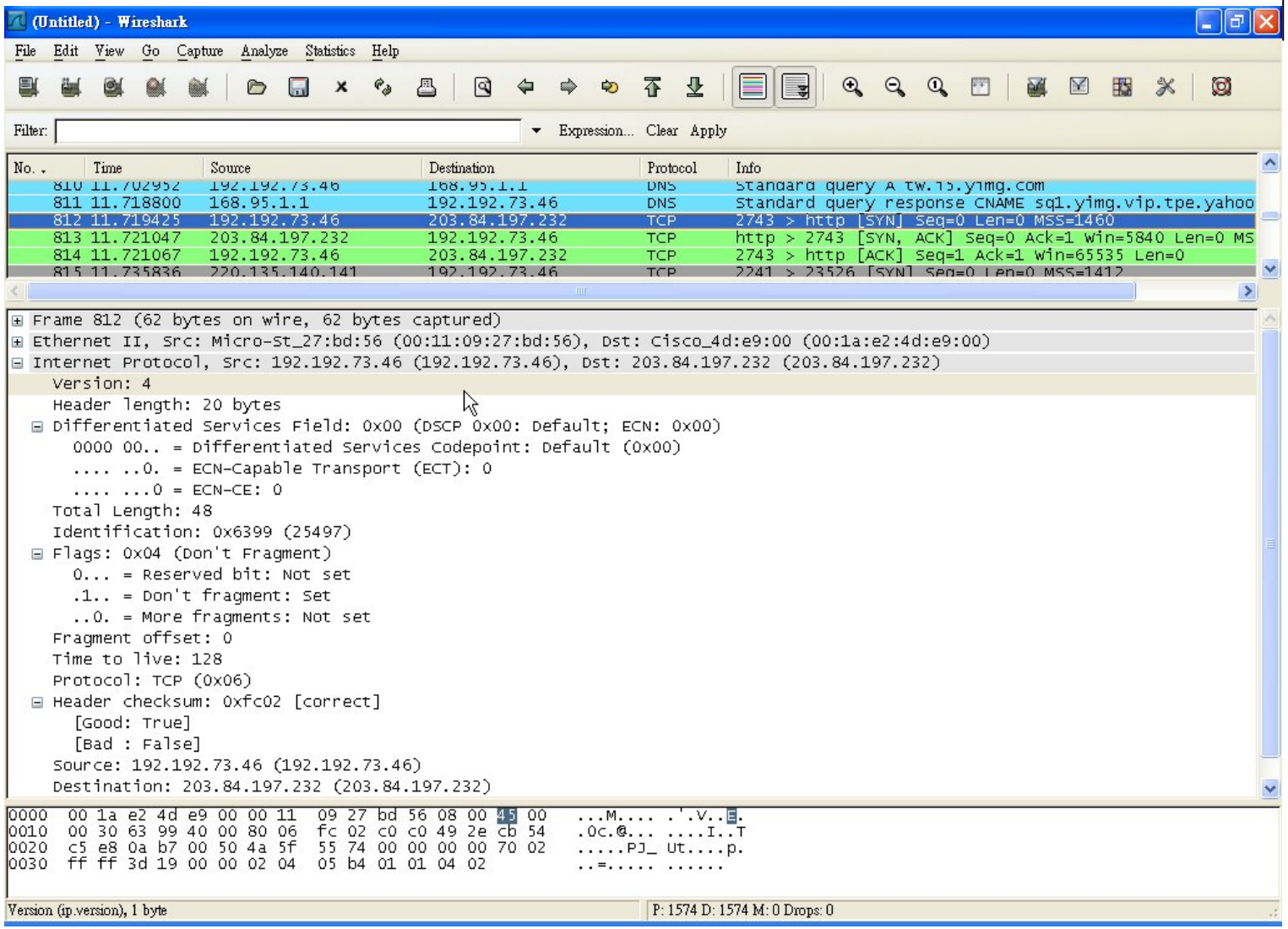


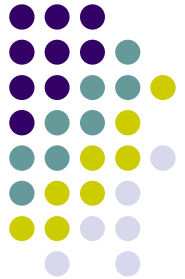
# IPv6



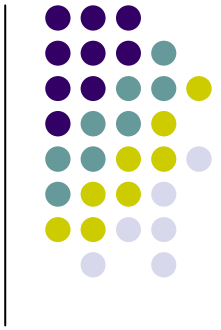

- 表頭(Header)： 記錄版本、位址、路由和長度等資訊， 長度固定為40Bytes。
- 延伸表頭（Extension Header）：延伸表頭並非必要的部份，只在有需要時才會存在。
- Payload：載送上層協定的資料。

# 實驗方法：擷取封包


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
811 11.718800 168.95.1.1 192.192.73.46 DNS Standard query response CNAME sq1.yimg.vip.tpe.yahoo
812 11.719425 192.192.73.46 203.84.197.232 TCP 2743 > http [SYN] Seq=0 Len=0 MSS=1460
813 11.721047 203.84.197.232 192.192.73.46 TCP http > 2743 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS
814 11.721067 192.192.73.46 203.84.197.232 TCP 2743 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
Frame 812 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: Micro-St_27:bd:56 (00:11:09:27:bd:56), Dst: Cisco_4d:e9:00 (00:1a:e2:4d:e9:00)
Internet Protocol, Src: 192.192.73.46 (192.192.73.46), Dst: 203.84.197.232 (203.84.197.232)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 48
Identification: 0x6399 (25497)
Flags: 0x04 (Don't Fragment)
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0xfc02 [correct]
[Good: True]
[Bad : False]
Source: 192.192.73.46 (192.192.73.46)
Destination: 203.84.197.232 (203.84.197.232)
0000 00 1a e2 4d e9 00 00 11 09 27 bd 56 08 00 45 00
0010 00 30 63 99 40 00 80 06 fc 02 c0 c0 49 2e cb 54
0020 c5 e8 0a b7 00 50 4a 5f 55 74 00 00 00 00 70 02
0030 ff ff 3d 19 00 00 02 04 05 b4 01 01 04 02
Version (ip.version), 1 byte
P: 1574 D: 1574 M: 0 Drops: 0



- **Version/Header Length:0x45**：第一個欄位值為4，指採用第四版的IP協定（IPV4）；第二個欄位值為5，表示此IP表頭的長度為5x4=20 Bytes。
- **Differentiated services Field (Type of Service):0x00**：服務類型值為00（十六進位），表示期望在一般優先權、一般延遲、一般通訊量、一般可靠度及一般成本下進行通訊。
- **Total Length:  48 bytes**：表示該封包的長度為48 Bytes，扣掉IP表頭的20 Bytes，資料長度有28 Bytes。



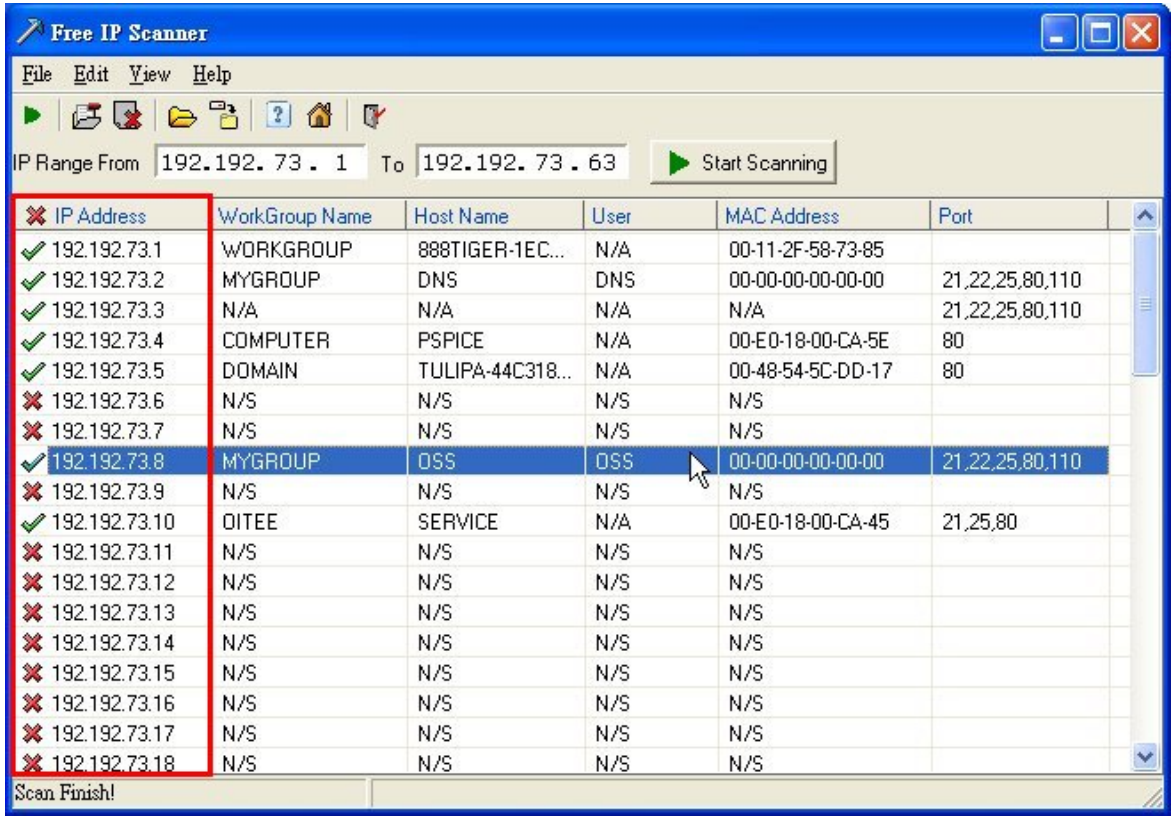
- **Ientification:25497**：表示該封包的識別代碼是225497。
- **Flags/Fragment Offset:0x4000**：
  - : 0... .... .... .... Not Used
  - : .1.. .... .... .... Don't Fragment
  - : ..0. .... .... .... Last Fragment
  - : ...0 0000 0000 0000 Fragment Offset: 0 bytes

  表示此封包未經過切割，Fragment Offset為0。
- **Time to Live: 128**：表示此封包在路由器之間轉送的次數。

- **Protocol ID:6 (TCP)**：表示此封包的傳輸型態為TCP協定。
- **Header CheckSum:0xfc02 [Correct]**：為IP表頭的HC檢查碼。
- **Source Address:192.192.73.46**：代表來源端的IP位址（192.192.73.46）。
- **Destination Address:203.84.197.232**：代表目的端的IP位址（203.84.197.232）。

# IP scanner (網路掃瞄)

- 使用Free IP scanner掃瞄192.192.73.1~192.192.73.63上所有IP機器的使用情況，其中代表使用這IP的機器是在開啟狀態，其中代表使用這IP的機器是在關閉狀態的。



# 本章註解

1. 網際網路是屬層層負責，或說層層不負責，即使你設TOS，只要連線中任一路由器不理會你，就沒有任何用途了，所以擷取的封包中Differentiated services Field (Type of Service)均為0x00。
2. 實際上IP雖然支援切割與重組機制，但事實上由於IP層無法具有封包重送的機制，現實上這些功能在TCP層會加以處理，IP層不會遇到需要切割與重組的機會，所以擷取的封包中Flags/Fragment Offset:0x4000應該都是0x4000。

# 學習評量

1. 請簡述網際網路發展史。
2. 請說明IP協定位於OSI網路協定的第幾層？
3. 請說明哪一個組織負責分配IP位址？如何分P位址？
4. 何謂動態IP位址、行動IP位址？
5. 何謂網域位址、廣播位址，主要功能為何？
6. 請說明連接導向式（Connection-Oriented）與非連接導向式（Connectionless）在效能和管理上有何差別？
7. 除書上列出的保留IP位址外，還有哪些IP位址是保留的？
8. 請說明TOS可對應至哪些網路服務？
9. 請說明IPv4和IPv6的差異處。
10. 說明IPv6如何利用IPv4網路傳送。