第四章 TCP/IP 協定與分析

4-1 Ethernet II 協定與分析

4-1-1 Ethernet 網路概述

早期 Ethernet 網路是採用 CSMA/CD (IEEE 802.3) 協定建構而成，係在匯流排的網路架構上協議主機之間存取傳輸媒介的協定(如圖 4-1 所示)。

- 協議傳送次序：廣播方式(CSMA/CD 協定)。
- 辨識工作站：Ethernet Address。
- Ethernet (10 Mbps)、Fast Ethernet (100 Mbps)、Gigabit Ethernet (1 Gbps)。

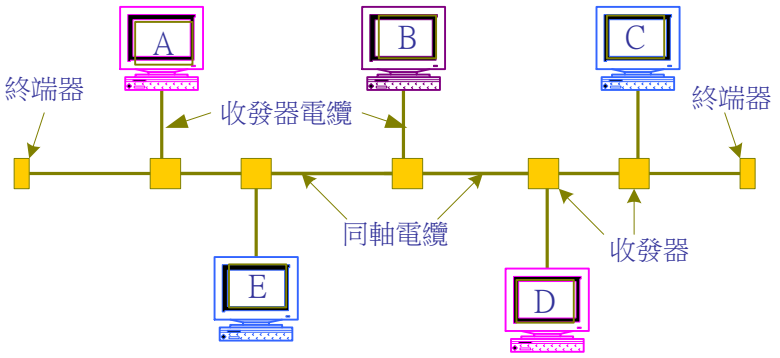


圖 4-1 傳統 Ethernet 網路架構

但隨著時代的演變，幾乎沒有共用匯流排的傳輸網路，大多採用集中式分配的集線器(HUB)或交換器(Switch)，傳輸媒介也不再是同軸電纜，也都採用絞對線(Cat 5 UTP)或光纖纜線的網路架構(如圖 4-2)。雖然各種裝置變化很大，但在發展過程中，為了向下相容必須保留舊裝置與新設備之中能共同運作，基本原則還是不能改變，最重要的是**『最小訊框』為 64 位元組，『最大訊框』為 1518 位元組**，的規範。

- 廣播方式：Hub。
- 交換轉送：Switch。

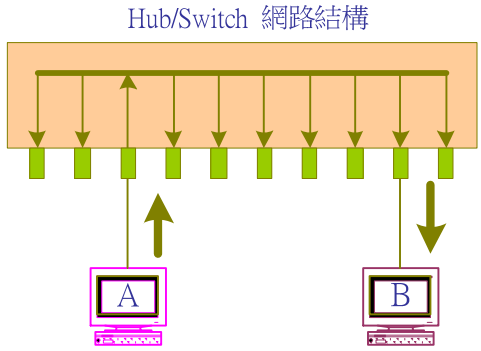


圖 4-2 集中式 Ethernet 網路架構

4-1-2 Ethernet II 封包格式

又從另一角度而言，早期網路還未成氣候時，大家一致認為 OSI 網路模型會成為未來的主流。發展 Ethernet 網路時也考慮了這一點，它必須連結上一層的 LLC(Logical Link Control) 協定，許多規範也依此而設定。真沒想到簡易的 TCP/IP 取代了繁複嚴謹的 OSI 協定，Ethernet 網路大多建立在 IP 協定上，不再是 LLC 協定。因此，ITE 簡化了 Ethernet 封包成為 Ethernet II (RFC 894) 封包格式，如圖 4-3 所示。

- 訊框長度：1518 Byte(訊息：~ 1500 Byte)
- 訊框傳送目的位址：DA (Destination Address)
- 訊框來源位址：SA (Source Address)
- 訊框承載訊息格式：Type(0800、0806、0835)
- 訊框承載訊息：IP、ARP、RARP、、、。

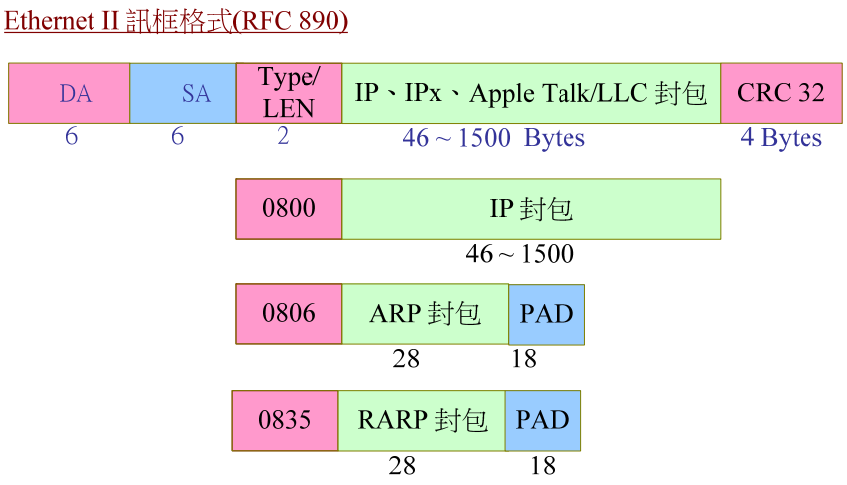


圖 4-3 Ethernet II 封包格式

其中最大的變革是將 LEN 欄位增加 Type 的功能，如果該欄位大 0x0800 則表示該訊框為 Ethernet II，所乘載 IP 或其他協定；否則為 Ethernet I 訊框，保留以後可能乘載 LLC 資料。即是 LEN/Type 欄位小於 0x0800 則是 LEN(Length) 功能，表示所乘載訊息的長度大小。如果大於 0x0800 則是 Type 功能，表示所乘載的協定如何，如 0x0800 則承載 IP 封包、0x0806 則是 ARP 封包等等，其他協定請查詢 RFC 894 規範。

4-1-3 Ethernet II 擷取與分析 - Wireshark

(A) 系統分析

一般區域網路皆是 Ethernet 網路，傳送訊息也都利用 Ethernet II 訊框包裝，我們只要在主機(Windows 7)執行一個網路命令，再利用封包擷取工具捕捉到任何封包，即可拿來分析(如圖 4-4)。

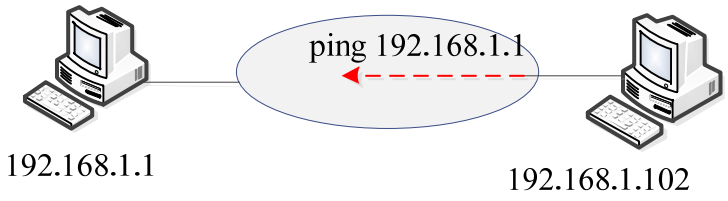


圖 4-4 Ethernet II 訊框擷取

(B) 封包擷取工具

我們需要用到下列工具：

- Wireshark 網路封包分析器(安裝於 Windows 7)
- Windows 命令提示字元：> ping 192.168.1.1 命令，使它產生網路訊息，再擷取得到。

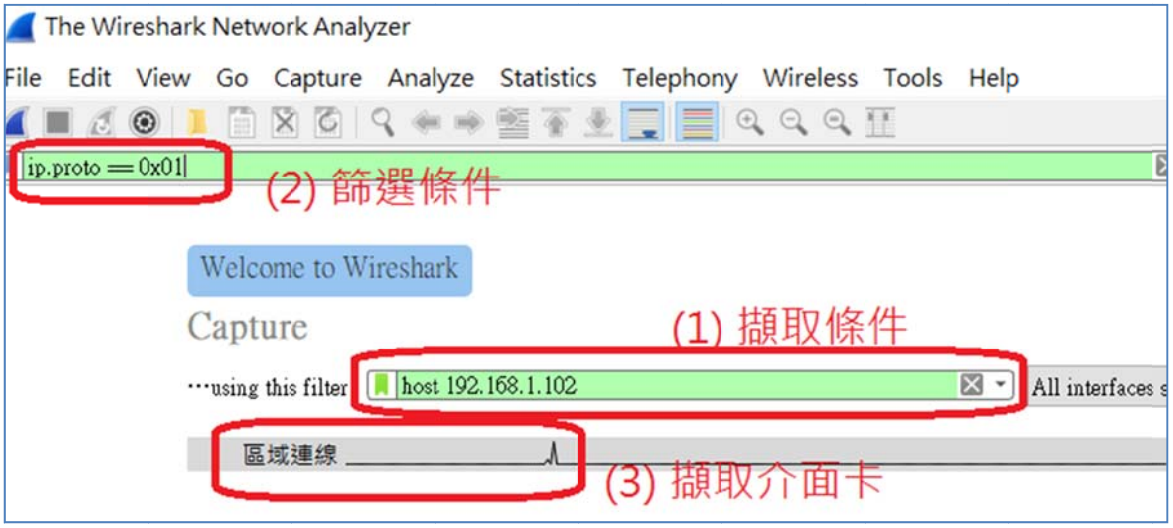
(C) 擷取封包步驟

(1) 開啟 Wireshark：

- **步驟 1：** 擷取條件= host 192.168.1.102。表示擷取到與主機位址 192.168.1.102 有關的封包。

步驟 2：篩選條件：ip.proto == 0x01(ICMP 封包)。擷取到與 192.168.1.102 主機有關的封包也許非常多，僅過濾篩選 IP 封包標頭內，protocol = 0x01 的封包，也就是僅過濾 IP 訊息欄位乘載 ICMP 的封包。

步驟 3：所欲擷取的介面卡，一般 Windows 7 主機只有一只介面卡，將它『按』兩下，則開始擷取封包，如下：

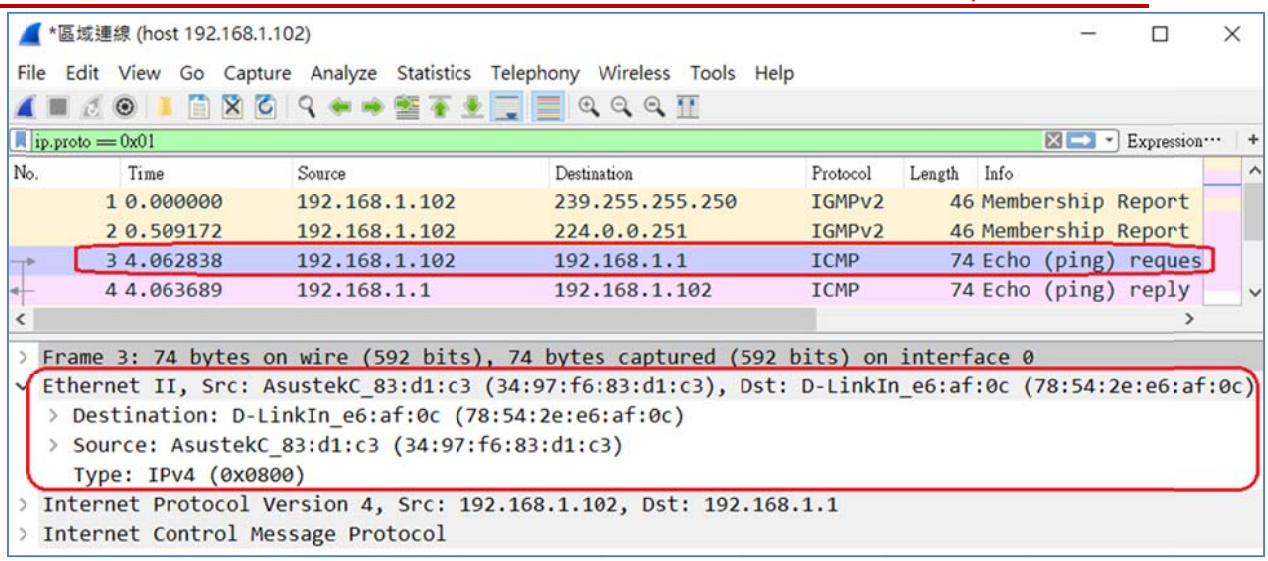


(2) 開啟 Windows 命令提示字元，執行 **> ping 192.168.1.1**，執行後，主機立即產生 ICMP 封包，Wireshark 平台上開始產生擷取結果。

(3) 如認為已擷取到所要的封包，則立即在 Wireshark 視窗按『**暫停**』按鈕，即可開始分析所擷取到的封包。

(D) Ethernet II 協定分析

擷取到封包如下圖所示，選擇 ICMP 封包(序號 3)，由協定分析視窗中點選 Ethernet II 訊息內容，可觀察出各個欄位內容如下：



- Destination：78:54:2e:e6:af:0c。目的主機的 Ethernet Address。
- Source：34:97:f6:83:d1:cs。來源主機的 Ethernet Address。
- Type:IPv4 (0x0800)。LEN/Type 欄位內容是 0x0800，表示承載 IP 封包。

至於其他欄位的內容(IP 與 ICMP)，接下來有其他範例分析。

4-1-4 Ethernet II 擷取與分析 – Packet Tracer

(A) 系統分析

一般區域網路皆是 Ethernet 網路，傳送訊息也都利用 Ethernet II 訊框包裝，我們只要在主機執行一個網路命令(如 ping 命令)，再擷取任何封包(ICMP 封包)，即可拿來分析。

(B) 網路規劃

吾人利用 Packet Tracer 設計一個簡單網路，包含有三個 PC 電腦，期望網路環境如下：

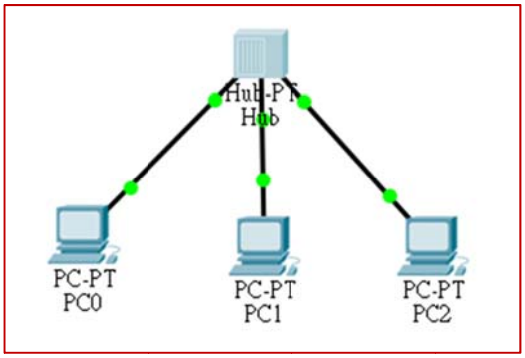
網路區段	Gateway/DNS	名稱	IP 位址	連接埠口
192.168.0.0/ 255.255.255.0	192.168.0.254/ 168.95.1.1	PC0	192.168.0.1	HUB(Fa0)
		PC1	192.168.0.2	HUB(Fa1)
		PC2	192.168.0.3	HUB(Fa2)

因此，我們需要在 Packet Tracer 上選擇下列裝置：

(1) Hub-PT：模擬集線器 (Hub) 一只。提供 PC 電腦之間連線。

(2) PC-PT：模擬 PC 主機三只。PC0 ~ PC2 主機使用。

(3) 規劃網路如下：**(請下載 Ethernet 封包擷取.pkt)**

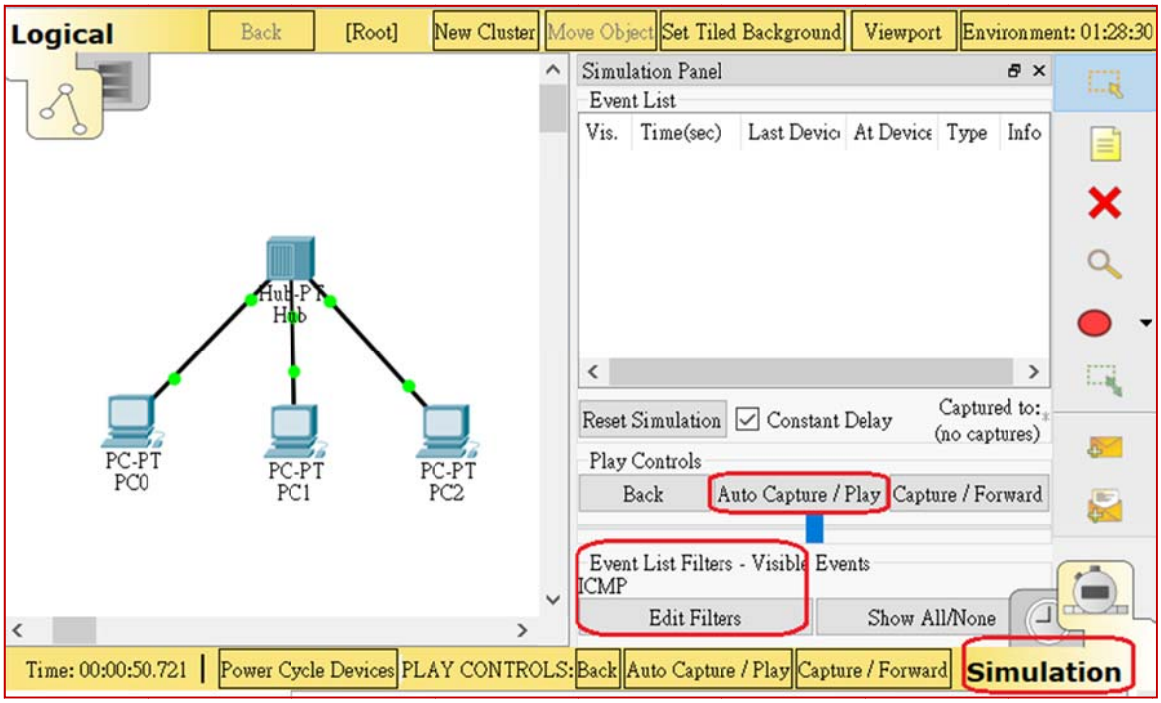


(C) 網路設定

- 集線器 Hub 不需任何設定。
- PC0 ~ PC2 須設定相關網路參數，如下(如 PC0)：Gateway = 192.168.0.254、DBS Server = 168.95.1.1、IP Address = 192.168.0.1、Subnet Mask = 255.255.255.0。

(D) 擷取封包步驟

(1) 步驟 1：Packet Tracer 採用 Simulation 模式，編輯 Edit Filters ，點選 ICMP，表示只擷取 ICMP 封包。



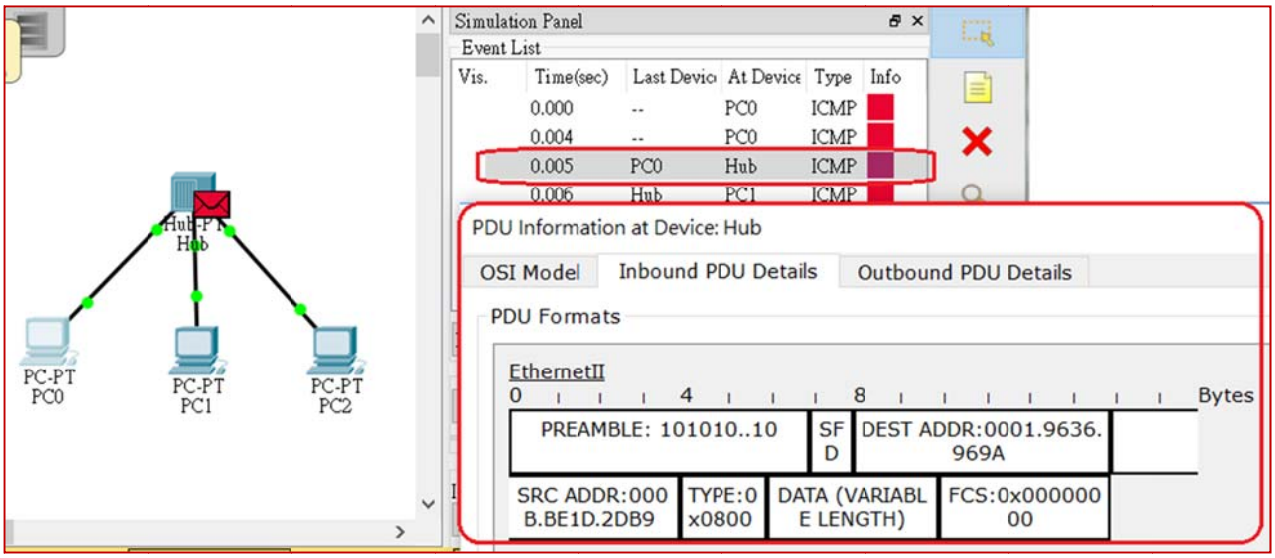
(2) 步驟 2：再由 PC0 上 ping 發送給 PC2 如下：(點選 PC0 -> Desktop -> Command Prompt ->)

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
```

(3) 步驟 3：在 packet Tracer 上按『Auto Capture/Play』暫停。

(E) Ethernet II 協定分析

(1) 步驟 1：在 Packet Tracer 按『Auto Capture/Play』，則可觀察到擷取到 ICMP 的封包，此訊息是表示在交換器上擷取到的，LastDevice 表示進入的；At Devices 表示出去到達的裝置。



(2) 步驟 2：分析 Ethernet II 封包標頭，如下。

- Destination：001.9636.969A。目的主機的 Ethernet Address。
- Source：000B.BE1D.2D89。來源主機的 Ethernet Address。
- Type:IPv4 (0x0800)。LEN/Type 欄位內容是 0x0800，表示承載 IP 封包。

4-2 ARP 協定與分析

4-2-1 ARP 協定概述

基本上，在 Ethernet 網路上傳送訊息，都必須以 Ethernet 封包格式封裝，來源位址與目的位址也都必須是 Ethernet Address 格式(48 bits)。但在 TCP/IP 網路上傳送訊息又都以 IP Address 格式(32 bits)，那 Ethernet 與 IP 位址之間的轉換機制，則須仰賴 ARP 協定來達成。

『位址解析協定』(Address Resolution Protocol, ARP) 是被用來以 IP 位址查詢其相對應的 Ethernet 位址，其運作方式如下圖所示。首先主機 A (163.15.2.1) 欲透過 Ethernet 網路傳送訊息給 IP = 163.15.2.4 主機，則發送出 ARP Request (查問 163.15.2.4) 廣播到所屬網路區段內。所有主機都會接收到該 ARP Request 封包，並分解是否詢問自己，如果不是就不予理會而拋棄。主機 C(163.15.2.4)收到 ARP Request 後，發現詢問自己則回應 ARP Reply (包含 Ethernet 位址) 給發問者(163.15.2.1)。 重點說明如下：

- Ethernet Address：主機在實體網路間識別。
- IP Address：主機在網際網路間識別。
- ARP Request：廣播方式。主機利用對方的 IP Address 詢問它的 Ethernet Address。
- ARP Reply：被詢問者回應 IP 與 Ethernet Address 對應給詢問者。
- ARP Cache：主機將詢問過的 Ethernet Address 與 IP Address 對應結果儲存，下次不用再問。

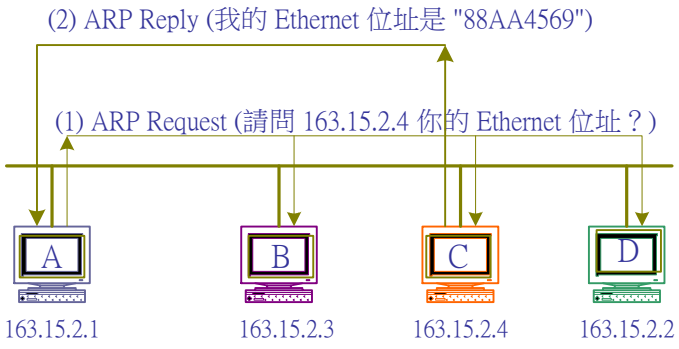


圖 4-5 ARP 運作方式

在 TCP/IP 規範裡還有**『反向位址解析協定』(Reverse Address Resolution Protocol, RARP)**，功能是由自己的 Ethernet Address 詢問自己應有的 IP Address，大多應用在動態 IP

設定使用，回應者是 RARP Server。但目前網路上大多使用 DHCP 與 Bootp 協定取代，已甚少使用 RARP 協定，因此本書不再敘述。但會另外介紹 DHCP 協定與服務。

ARP Request 與 ARP Reply 封包 (如圖 4-6) 大致相同，各欄位功能如下：

- **Hardware Type**：表示發送主機使用之網路實體介面種類，如 1 表示 Ethernet 網路介面。
- **Protocol Type**：表示所使用的通訊協定，如 0x0800 表示 IP 協定，其它通訊協定模式如表 5-1 所示。
- **Operation Type**：表示此封包的工作模式：

  1 → ARP 要求（ARP Request）

  2 → ARP 回應（ARP Reply）

  3 → RARP 要求（RARP Request）。

  4 → RARP 回應（RARP Reply）
- **HLEN**：網路介面卡硬體位址長度。若 Ethernet 位址的長度為 6。
- **PLEN**：網路協定位址長度。因為 IP 位址長 4 個位元組，此值為 4。
- **Sender HW**：發送端的硬體位址。如果是 Ethernet 網路的話，此為 6 個位元組長的地址，如 0x8823AA112233。
- **Target HW**：目的地的硬體位址。
- **Sender IP**：發送端的 IP 位址，如 163.15.2.1。
- **Target IP**：目的地主機的 IP 位址，如 163.15.2.4。

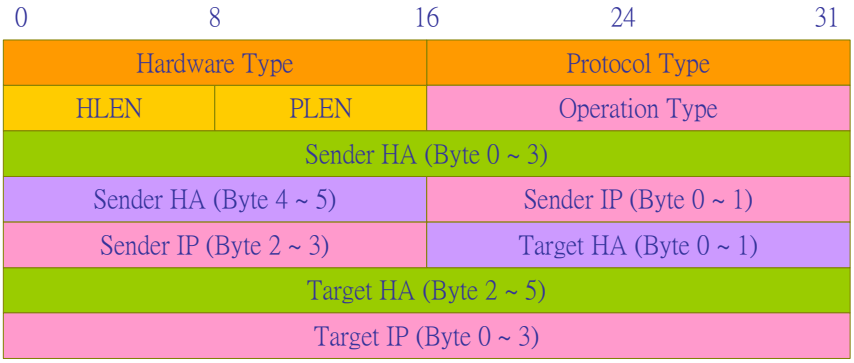


圖 4-6 ARP 封包格式

4-2-2 ARP 擷取與分析 - Wireshark

(A) 系統分析

ARP 封包是當工作站欲詢問某一 IP 位址是屬於哪一個工作站所有，並請它回應相對應的 Ethernet 位址，因此它是屬於廣播訊息。查詢後工作站會將查詢結果存放於主機的 ARP 佇列(ARP Cache) 內，就不須重複查詢了。因此，我們擷取之前先將 ARP Cache 清除掉，再隨意發送一個封包給某一主機，便會發生 ARP 封包，再擷取它即可。

吾人利用本機(120.118.165.107) 執行 ping 命令，對一個不知 Ethernet 位址的電腦 (IP = 120,118.165.191)，讓他自動產生 ARP 查詢訊息，如圖 4-7 所示。

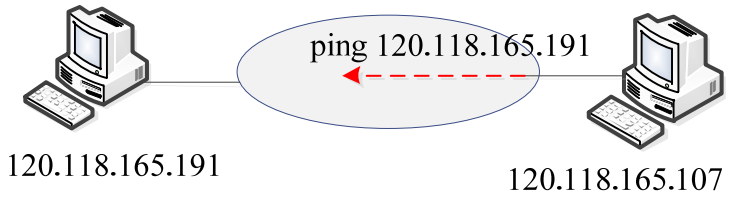


圖 4-7 ARP 封包攫取

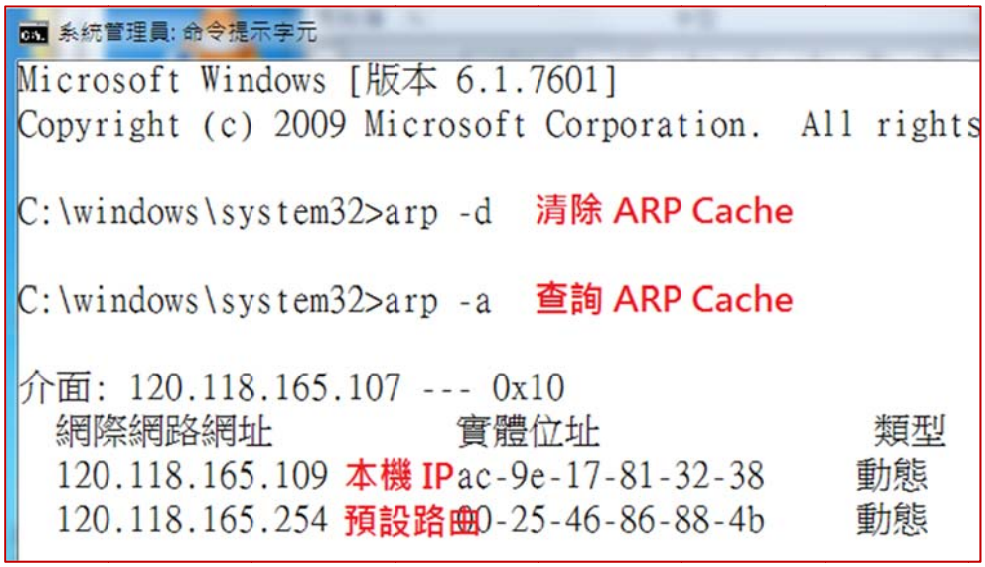
(C) 擷取封包工具

我們需要用到下列工具：

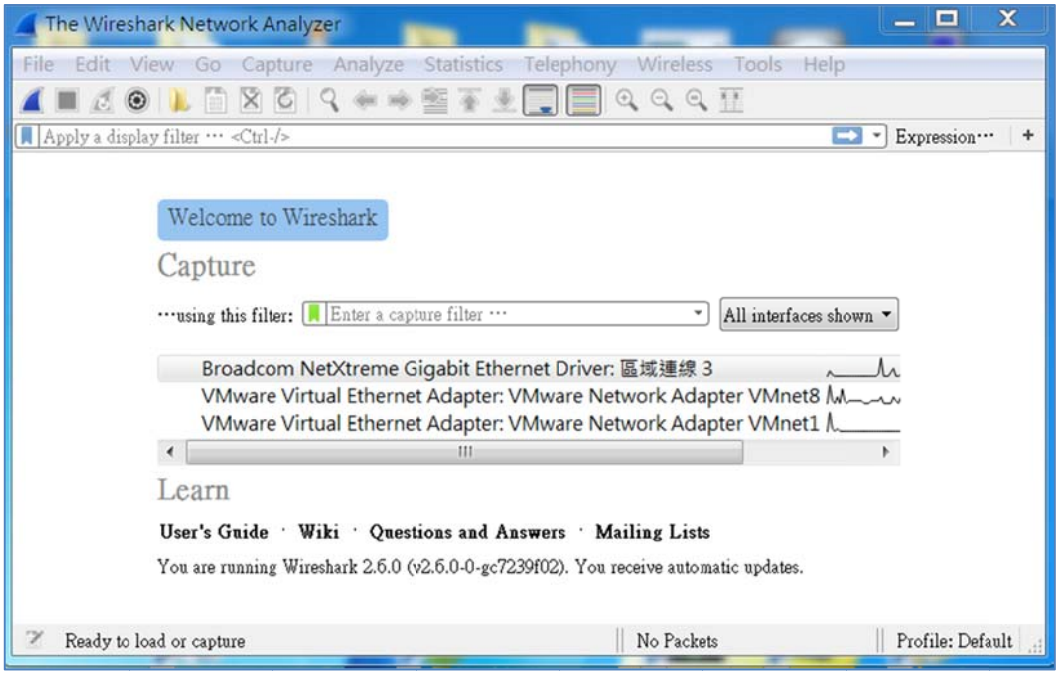
- Wireshark 網路封包分析器(安裝於 Windows 7)。
- Windows 命令提示字元：ipconfig、arp、ping 等命令。

(D) 擷取封包步驟

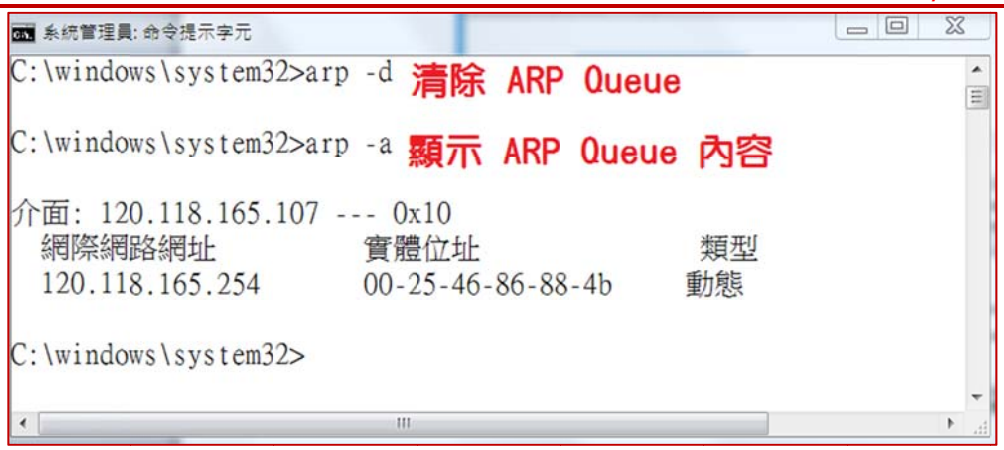
(1) 開啟 Windows 命令提示字元(**利用管理員身分開啟**)，首先利用 ipconfig 命令查詢本電腦的 IP 位址(查出為 **120.118.165.107**)，再執行 **arp –d** 與 **arp –a** 等命令，清除電腦內記憶的 ARP 訊息。



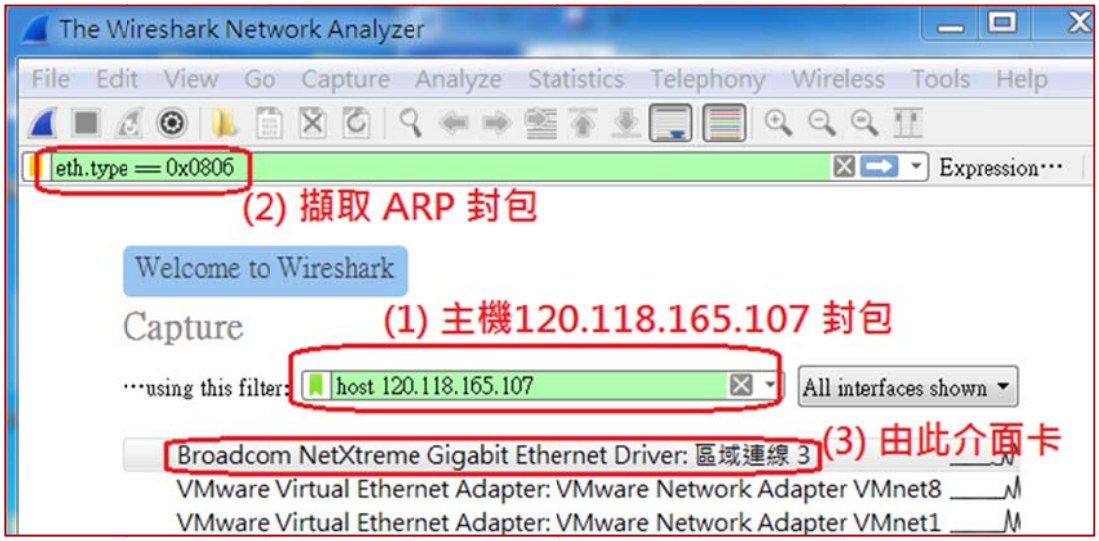
(2) 開啟 Wireshark



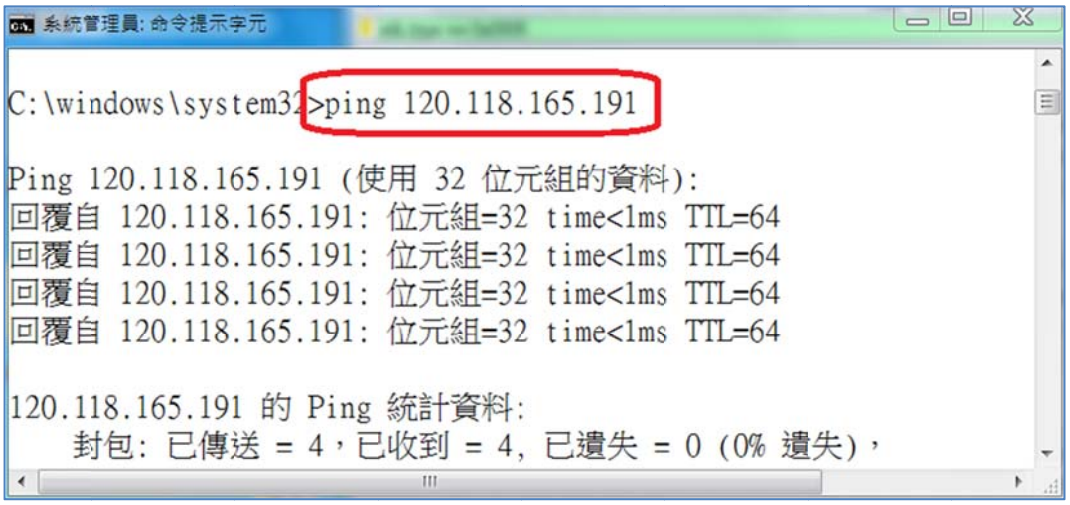
(2) 開啟 Windows 命令提示字元(**利用管理員身分開啟**)，首先利用 ipconfig 命令查詢本電腦的 IP 位址(查出為 **120.118.165.107**)，再執行 **arp –d** 與 **arp –a** 等命令，清除電腦內記憶的 ARP 訊息。



(2) 選擇 Wireshark 擷取篩選項目(host 120.118.165.107)與 eth.type = 0x0806 表過濾 ARP 封包，再選擇介面卡，如下：



(3) 此時 Wireshark 已開始擷取封包，吾人立即在 Windows 命令提示字元上執行：ping 某一主機位址(ping 120.118.165.191)使它產生 ARP 封包(ARP cache 已清除)，如下：



(4) 在 Wireshark 視窗按暫停，並在顯示篩選器上選擇 arp，如下：

(E) ARP 協定分析

在 Wireshark 視窗按暫停，分析 ARP Request 與 ARP Reply 封包如下：

(E-1) ARP Request 封包分析

由上圖中第 141 封包是主機發送出去 ARP request 封包，點選該封包由協定視窗上可以看出各個封包標頭的內容。

```
Frame 141: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   Source: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17)
   Type: ARP (0x0806)
Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: HewlettP_0a:c1:17 (00:25:b3:0a:c1:17)
   Sender IP address: 120.118.165.107
   Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
   Target IP address: 120.118.165.191
```

- Ethernet II 封包標頭，如下：
  - DA：目的位址。廣播位址(broadcast)
  - SA(Source)：來源位址。00:25:b3:0a:c1:17(48 bits)
  - Type：0x0806 表 ARP 封包。

DA	SA	0806	ARP封包	PAD	CRC32
6	6	2	28	18	4 Bytes

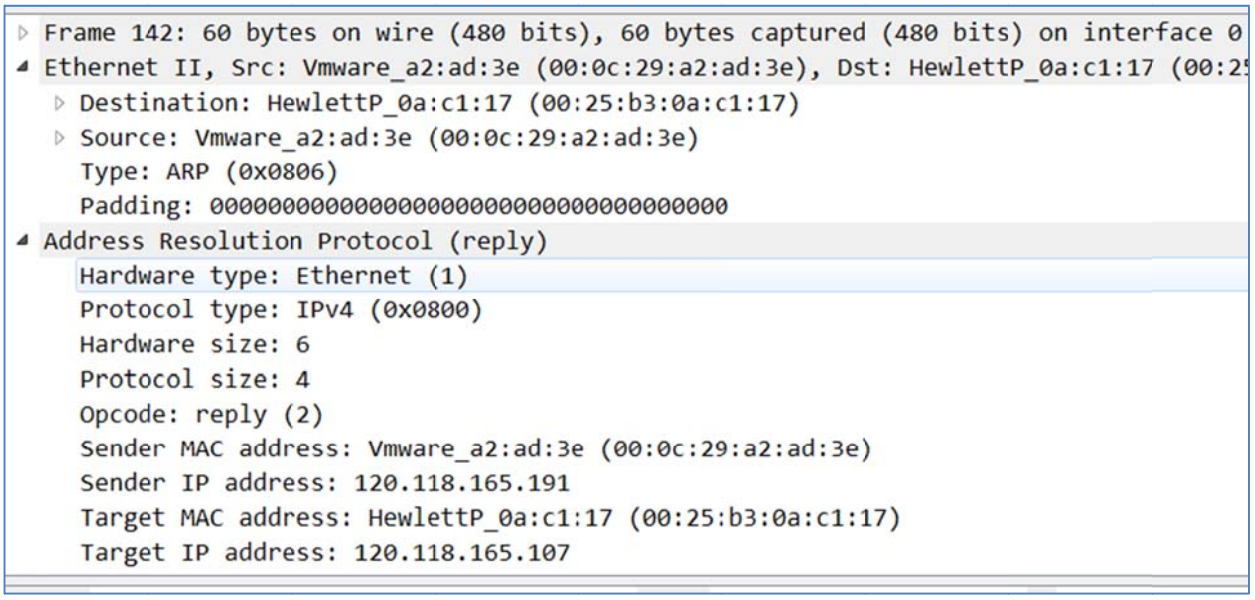
- ARP request 封包標頭，如下：

0	8	16	24	31
Hardware Type			Protocol Type	
HLEN	PLEN		Operation Type	
Sender HA (Byte 0 ~ 3)				
Sender HA (Byte 4 ~ 5)			Sender IP (Byte 0 ~ 1)	
Sender IP (Byte 2 ~ 3)			Target HA (Byte 0 ~ 1)	
Target HA (Byte 2 ~ 5)				
Target IP (Byte 0 ~ 3)				

- Hardware type：Ethernet (I)。
- Protocol type：IPv4。
- Hardware size：6。
- Protocol type：4。
- Opcode：Request (1)。
- Source MAC address：00:25:b3:0a:c1:17。
- Source IP address：120.118.165.107。
- Target MAC address：00:00:00:00:00:00。
- Target IP address：120.118.165.191

(E-2) ARP Reply 封包分析

由上圖中第 142 封包是 120.118.165.191 主機回覆的 ARP respond 封包，點選該封包由協定視窗上可以看出各個封包標頭的內容。



- Ethernet II 封包標頭，如下：
  - Destination：00:25:b3:0a:c1:17。
  - Source：00:0c:29:a2:ad:3e
  - Type：0x0806 表 ARP 封包。
- ARP reply 封包標頭，如下：
  - Hardware type：Ethernet (I)。

- Protocol type：IPv4。
- Hardware size：6。
- Protocol type：4。
- Opcode：reply (2)。
- Source MAC address：00:0c:29:a2:ad:3e。
- Source IP address：120.118.165.191。
- Target MAC address：00:25:b3:0a:c1:17。
- Target IP address：120.118.165.107。

4-2-3 ARP 擷取與分析 – Packet Tracer

(A) 系統分析

ARP 封包是當工作站欲詢問某一 IP 位址是屬於哪一個工作站所有，並請它回應相對應的 Ethernet 位址，因此它是屬於廣播訊息。查詢後工作站會將查詢結果存放於主機的 ARP 佇列(ARP Cache) 內，就不須重複查詢了。因此，我們擷取之前先將 ARP Cache 清除掉，再隨意發送一個封包給某一主機，便會發生 ARP 封包，再擷取它即可。清除命令如下：

```
C:\>arp -a   [顯示 ARP Queue]

Internet Address Physical Address Type
192.168.0.2 0001.9636.969a dynamic


C:\>arp -d      [刪除 ARP Queue]
```

但 Packet Tracer 並沒有模擬 ARP Catch 的功能，我們只要執行 ping 命令，對一個不知 Ethernet 位址的電腦 (IP = 120,118.165.191)，讓他自動產生 ARP 查詢訊息即可。

(B) 網路規劃

吾人利用 Packet Tracer 設計一個簡單網路，包含有三個 PC 電腦，期望網路環境如下：

網路區段	Gateway/DNS	名稱	IP 位址	連接埠口

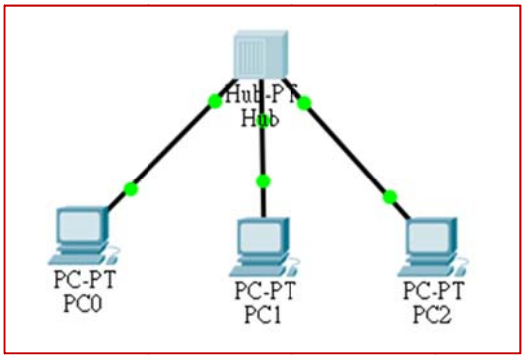
192.168.0.0/ 255.255.255.0	192.168.0.254/ 168.95.1.1	PC0	192.168.0.1	HUB(Fa0)
		PC1	192.168.0.2	HUB(Fa1)
		PC2	192.168.0.3	HUB(Fa2)

因此，我們需要在 Packet Tracer 上選擇下列裝置：

(1) Hub-PT：模擬集線器 (Hub) 一只。提供 PC 電腦之間連線。

(2) PC-PT：模擬 PC 主機三只。PC0 ~ PC2 主機使用。

(3) 規劃網路如下：**(請下載 ARP 封包擷取.pkt)**

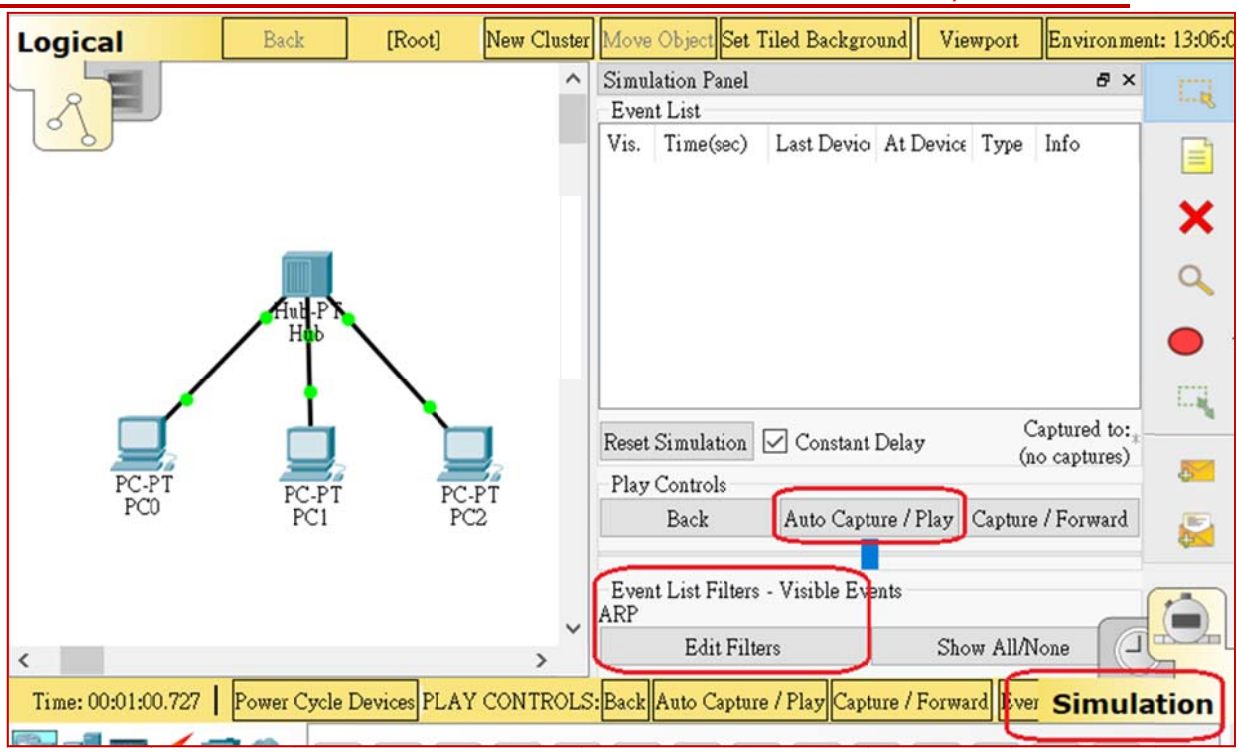


(C) 網路設定

- 集線器 Hub 不需任何設定。
- PC0 ~ PC3 須設定相關網路參數，如下(如 PC0)：Gateway = 192.168.0.254、DBS Server = 168.95.1.1、IP Address = 192.168.0.1、Subnet Mask = 255.255.255.0。

(D) 擷取封包步驟

(1) 步驟 1：Packet Tracer 採用 Simulation 模式，編輯 Edit Filters ，點選 ARP，表示只擷取 ARP 封包。



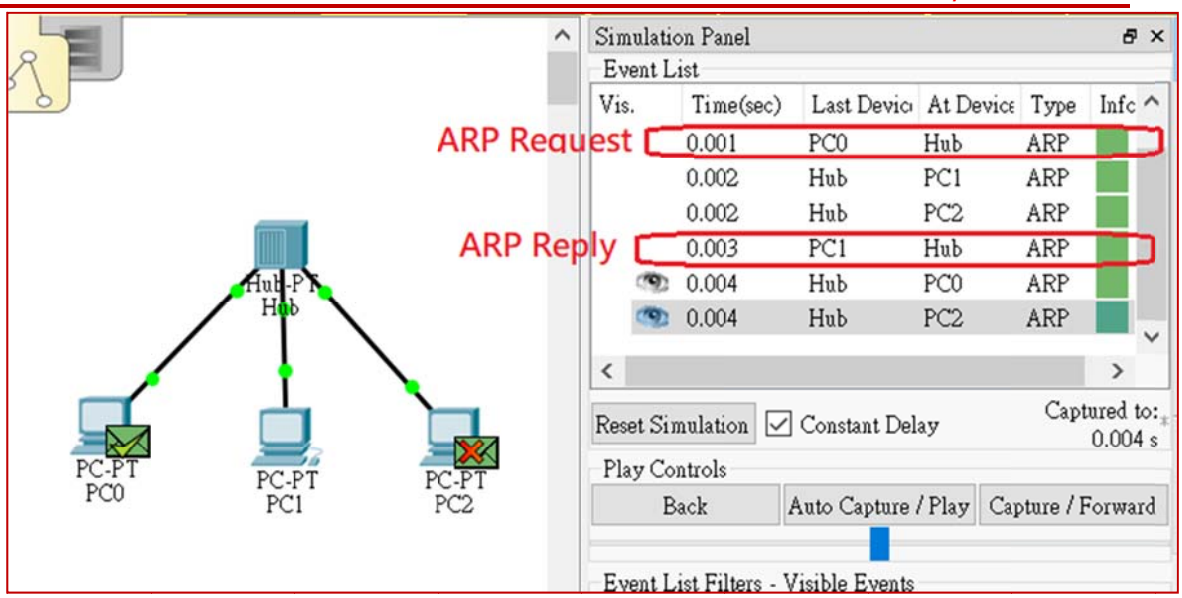
(2) 步驟 2：再由 PC0 上 ping 發送給 PC2 如下：(點選 PC0 -> Desktop -> Command Prompt ->)

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
```

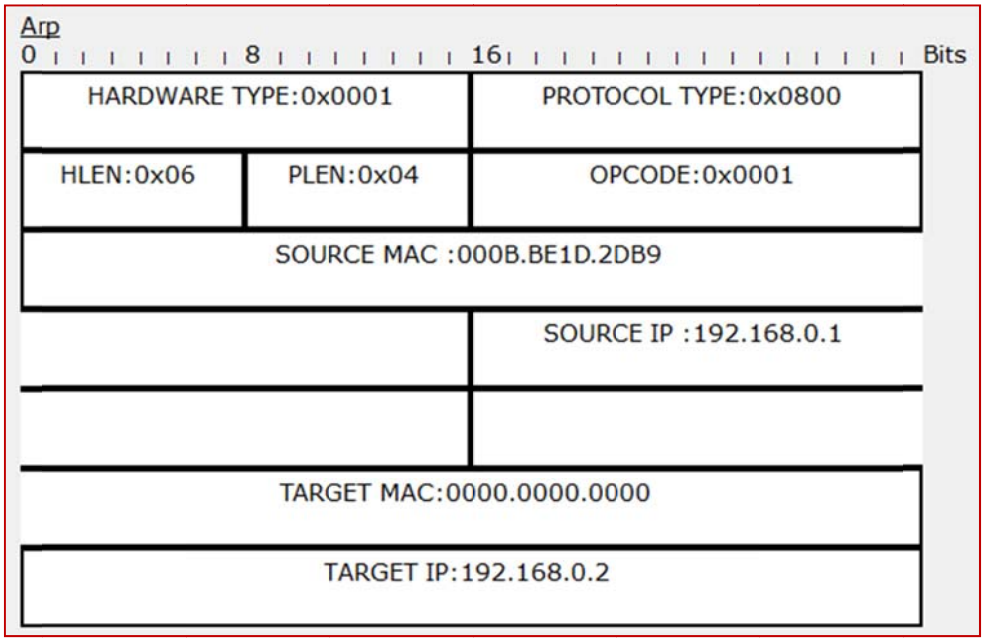
(3) 步驟 3：在 packet Tracer 上按『Auto Capture/Play』暫停。

(D) ARP 協定分析

(1) 步驟 1：在 Packet Tracer 按 『Auto Capture/Play』，則可觀察到擷取到 ARP 的封包，其中包含 ARP Request 與 ARP Reply 兩封包。

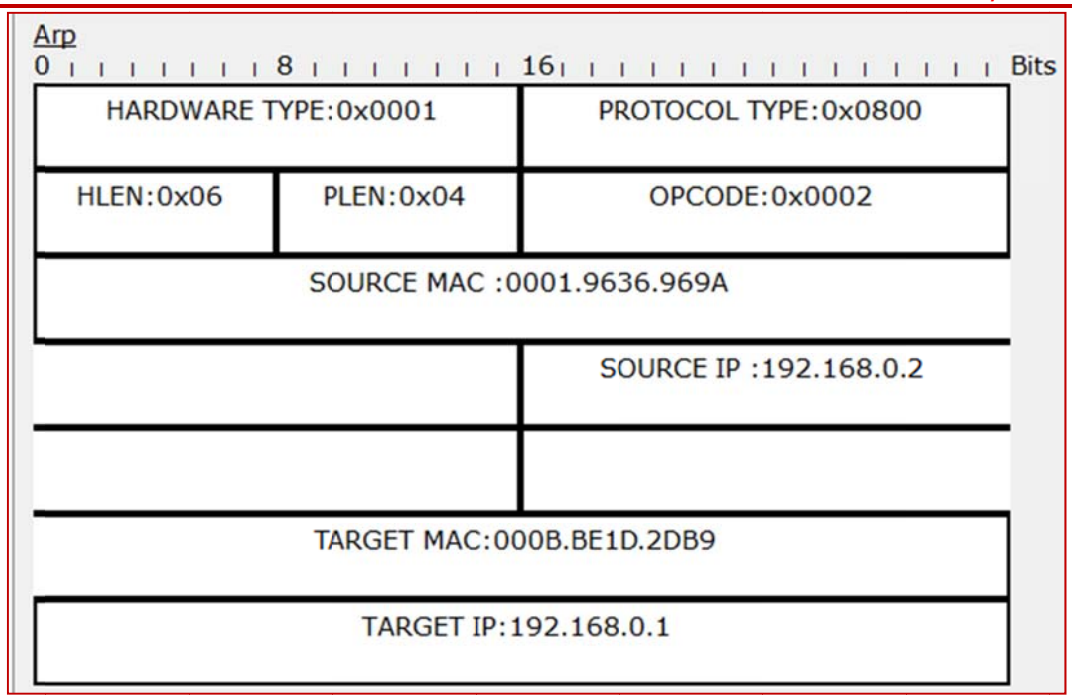


(2) 步驟 2：分析 ARP Request 封包標頭，如下：



- Hardware Type：0x0001、Protocol Type：0x0800、Opcode：0x0001。
- Source MAC 與 Source IP。
- Target MAC： 0、Target IP = 192.168.0.2。

(3) 步驟 3：分析 ARP Reply 封包標頭，如下：



- Hardware Type：0x0001、Protocol Type：0x0800、Opcode：0x0002。
- Source MAC = 0001.9636.969A 與 Source IP = 192.168.0.2。
- Target MAC：000B.BE1D.2DB9、Target IP = 192.168.0.1。

4-3 IP 封包與分析

4-3-1 IP 協定功能

IP 是 Internet 網路之中最主要的協定，功能是在廣泛複雜的網路上，如何尋找到所欲連接之工作站，並負責雙方的連線。IP 協定所採用的非連接方式的**『電報傳輸』(Datagram)**，主要的工作有二：(1) 每一部工作站如何去定名？使成為網路唯一的識別名稱，有了這個呼叫名稱，才可以連結其它工作站，或被其它工作站所連結，宛如電話號碼一般；(2) 如何尋找連結路徑？在廣泛複雜網路之中，如何尋找出可以到達目的地的最佳路徑。這裡有兩個重點必須釐清它：

(1) IP 位址。一個合法的 IP 位址是全網際網路上通用的，雖然它只有 32 bits，但絕對不可以重複。這與 Ethernet 位址有很大不同，它有 48 bits，但僅侷限於網路區段內不可重複。

(2) IP 繞路功能。IP 協定最大的功能是如何在廣泛的網際網路上，尋到所欲傳輸的目地位址所在位置，這就是 IP Routing 功能。它並非由某一裝置主導而成(集中控制型)，而是由訊息所經過的路由器(Router)共同協力而成(分散式控制型)。

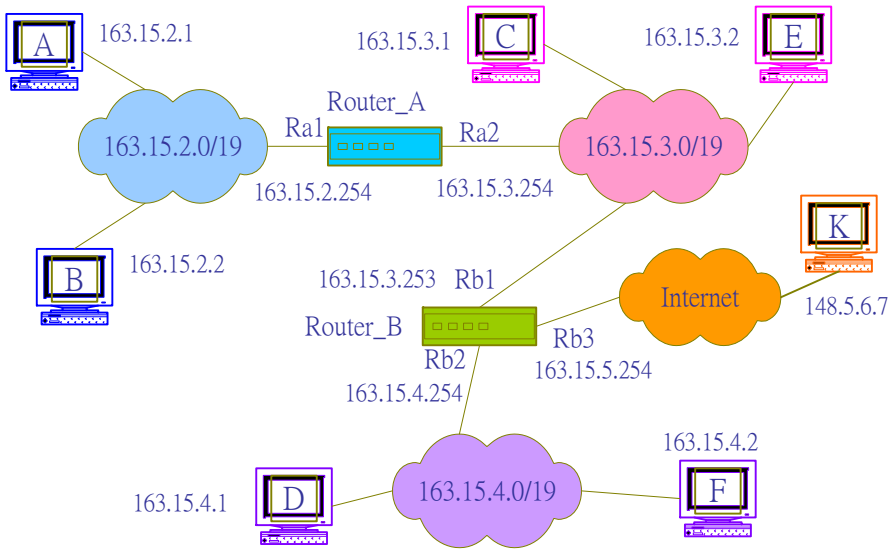


圖 4-7-1 路徑選擇

由此可見，IP 協定並非完全可靠的通訊模式，它的安全性必須仰賴上一層 TCP 協定來達成。

4-3-2 IP 位址與分級

(A) IP 位址結構

在 IP 網路中，任何一部連線的電腦或工作站設備都稱為主機（host）。早期 TCP/IP 被設計成適合在不同類型、位置之全球各地的電腦系統之間連接，為了方便標定每部主機，TCP/IP 定義了一套通用的定址方法。當時理想的定址格式必須能提供足夠的路徑選擇（routing）資訊，而且不要佔用太多記憶體空間，因此，將 IP 位址（IP Address）的長度設定為 32 位元。為方便表達，我們將此 32 位元分割成四段，連續 8 位元為一組，每組並以十進位值（0 ~ 255）表示，每組之間以點（dot）分隔。整個 IP 位主表示法就如下所示：

dec3.dec2.dec1.dec0（如 163.15.2.1）

雖然 IP 位址長為 32 位元，但其中包含兩種號碼：**網路號碼（Network number）**及**主機號碼（Host number）**，因此 IP 位址也可以表示成：(如圖 4-8 所示)

【network number, host number】

圖 4-8 IP 位址結構

在實務連接上，並非每一部主機上都只有一個 IP 位址，一般 IP 位址都依照網路介面卡（Ethernet 網路卡）設定。如主機有特殊需要安裝多個網路介面卡（如當路由器使用），每只網路介面卡上都必須設定一個 IP 位址，因此，一部主機上就擁有多個 IP 位址，同時也容許類似虛擬主機的設定，表示一只網路介面卡上可設定多個 IP 位址。

(B) IP 位址分級

在 32 位元長度的位址之中，應該多少位址長度來表示網路位址或主機位址。TCP/IP 網路依照所能容納的主機和網路的數量多寡分成 A、B、C 、D 和 E 五種類級（class），如圖 4-9 所示，其中 Class D 目前為實驗性多點廣播（Multicast）位址，Class E 則保留未來發展之用。分級技巧是配置不同數目的網路位址，網路位址的位元數愈多，所能指定的網路數量就愈多，但相對應的主機位址就愈少。Class C 所能容納的網路位址最多，所以在 Internet 網路上定址方式皆採用 Class C 模式。Class A 所能容納的主機位址最多，但相對應的所能容納的網路位址最少，一般使用在區域網路的定址模式。各類級的特性如下：

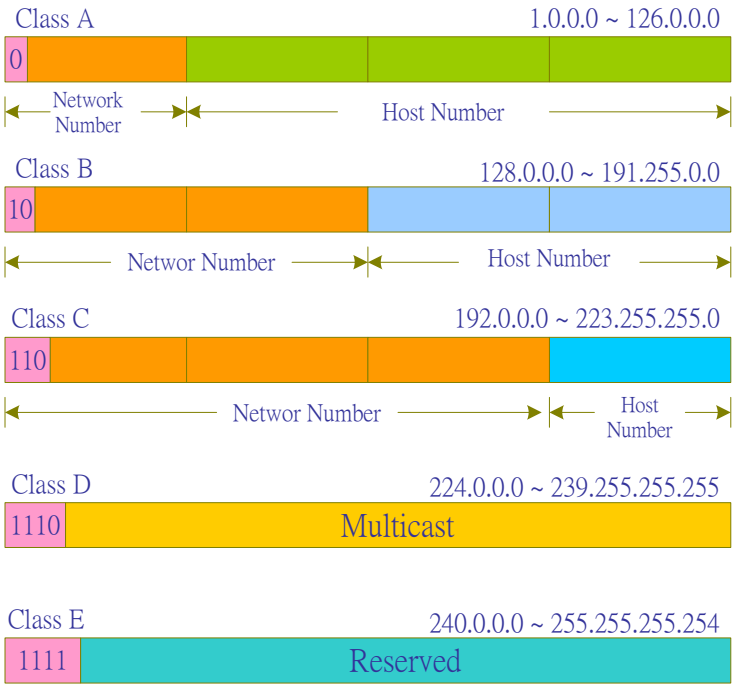


圖 4-9 各類級的 IP 位址結構

(1) Class A：以最高位元（第 31 位元）為 0 表示 Class A 模式。前一位元組（8 位元）表示網路位址；而後 24 位元表示主機位址。網路位址由 1.0.0.0 ~ 126.0.0.0，所能表示的主機位址是 1.0.0.0 ~ 126.255.255.255 的範圍之內。Netmask = 255.0.0.0（下小節說明）。

(2) Class B：以二個最高位元為 10 表示 Class B 模式。前 16 位元表示網路位址；而後 16 位元表示主機位址。網路位址由 128.0.0.0 ~ 191.255.0.0，所能表示的主機位址為 128.0.0.0 ~ 191.255.255.255 的範圍之內。Netmask = 255.255.0.0。

(3) Class C：以前三個最高位元為 110 表示 Class C 模式。前 24 位元是網路位址；而後 8 位元為主機位址。網路位址由 192.0.0.0 ~ 223.255.255.0，所能表示的主機位址為 192.0.0.0 ~ 223.255.255.255 的範圍之內。Netmask = 255.255.255.0。

(4) Class D：以前四個位元為 1110 表示 Class D 模式。其主要應用於多點廣播（Multicast），一些特殊應用軟體皆用此模式，來對某些定點（工作站）廣播，如隨選視訊（VOD）就用此定址模式，對若干個定點工作站廣播視訊。

(5) Class E：以前四個最高位元為 1111 表示 Class E 模式。目前保留尚未使用。

(C) 網路位址與主機位址

經過 IP 分級後，IP 位址可分為兩大部份：網路位址和主機位址。如以 Class B 中的 163.15.3.42 為例，此 IP 位址可區分為下列兩種位址：

- 網路位址：163.15.0.0
- 主機位址：0.0.3.42

如果僅由 IP 位址來觀察，如此分類好像不是很重要，但是在路徑選擇時就非常重要，因為一般路徑選擇只觀察網路位址，而不用理會主機位址是多少。

(D) 網路遮罩（Network Mask, Netmask）

IP 位址是由網路號碼和主機號碼組成的 32 位元，為方便起見，一般都用 [network#, host#] 表示。網路號碼決定主機所屬的網路位址，因此主機在傳遞封包之前，會先過濾出網

路號碼，再決定封包應該往哪一個網路傳送。為使能由 IP 位址中過濾出網路號碼，我們使用『**網路遮罩**』(**Netmask**) 來過濾。網路遮罩亦為 32 位元，在位元中 "1" 表示網路位址；而 "0" 表示主機位址，其遮罩方式如圖 4-10 所示。如 IP 分級方式，各等級之網路遮罩為：

- **Class A**：網路遮罩為 255.0.0.0
- **Class B**：網路遮罩為 255.255.0.0
- **Class C**：網路遮罩為 255.255.255.0

在一般網路遮罩，皆是 IP 位址的前面若干位元設定為 "1"，因此，我們以網路號碼的長度 (也是網路遮罩的長度) 來代表網路位址的範圍，以『**主機號碼/網路號碼長度**』來表示一個網路位址，如：

IP = 163.15.2.3/16 表示網路遮罩長度為 16 位元，則：

網路位址 = 163.15.0.0

主機位址 = 0.0.2.3

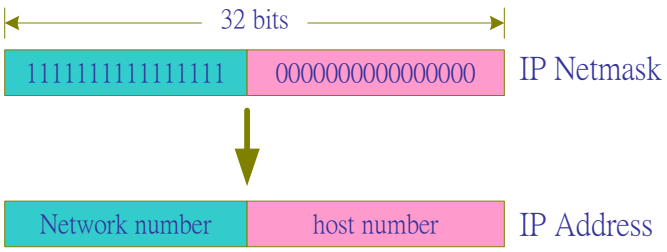


圖 4-10 IP Netmask

4-3-3 次網路位址

如果硬是將網路位址區分為三個類級(Class A ~ C)，恐怕很難滿足各種環境需求。例如，目前 TANet 使用 Class B 的定址模式，分配到每一個學校 2 ~3 個網路號碼。每一個學校裡的網路，是由多個系所的區域網路所構成，在技術上，每一個區域網路都要有一個網路號碼，因此網路號碼一定不符所需，這也是 IP 分級所衍生的問題。解決的方法就是再劃分次網路 (Subnet)，產生次網路的基本原理，是將原有主機號碼的幾個位元拿來當網路號碼，並沒有改變原來 32 位元的 IP 位址格式。

如欲劃分次網路，就必須有次網路的編號，原來 IP 位址所表達的是 [network#, host#] 方式，就必須更換為 [network#, subnet#, host#] 形式。而增加次網路號碼，就必須犧牲原來主機號碼的數量，次網路號碼增加愈多，主機號號碼就減少愈多。對整個位址格式並未改變，因為原來網路號碼並未改變，對外部網路而言，次網路位址也被視為主機位址，因此連結到外部網路並不影響。我們以一個例子說明，假使希望在 163.15.0.0 的網路上增加 8 個次網路，基本上，163.15.0.0/16 網路是屬於 Class B 格式，它原來的 IP Netmask 為 255.255.0.0。我們為了增加 8 個次網路，必須將 3 個位元的主機號碼拿來當次網路號碼，因此 Netmask 為 255.255.224.0，如圖 4-11 所示。

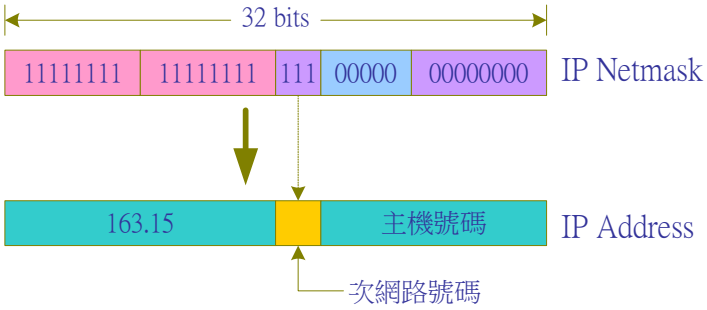


圖 4-11 次網路號碼

分割後所產生的網路位址為：(Network number = 163.15.0.0、Netmask = 255.255.224.0)

163.15.0.0/19、163.15.32.0/19、163.15.64.0/19、163.15.96.0/19、163.15.128.0/19、163.15.160.0/19、163.15.192.0/19、162.15.224.0/19。

4-3-4 IP 保留與私有位址

(A) 保留位址

除了上述 IP 分級外，還有一些網路位址保留為特殊使用，其它應用必需避免使用下列位址：

- **預定閘門 (Default Router)：**以網路 0 保留特殊使用，並以『**0.0.0.0**』作為預定閘門位址。
- **回繞位址 (Loopback Address)：**網路 127 也保留於特殊用途，並以『**127.0.0.0**』作為回繞位址，『**127.0.0.1**』表示主機位址，主要作為測試網路使用。

- **廣播位址（Broadcast Address）**：IP 位址全部為 1 時，表示是對所有主機的廣播位址『**255.255.255.255**』。一般應用上只對本網路廣播，因此，將所有主機位址設定為 1 時，表示對本網路所有主機管播，譬如，163.15.0.0 網路的廣播位址為『**163.15.255.255**』。

剛開始設計 TCP/IP 網路時，電腦還未普及，網路也非常少，TCP/IP 協定開始應用時也只連結大型主機，因此 32 位元容量的 IP 位址對當時來講已足足有餘。但沒有想到 Internet 網路大風行，理論上，任何一部電腦連結上 Internet 網路都需要一個獨一無二的 IP 位址，因此 IP 位址將會在短期內被耗盡。雖然目前已提出 IPv6 的解決方案，但要網路上使用中的路由器和主機都更新為 IPv6 的通訊協定，也並非易事。目前網路上大多透過『**網路位址轉換器**』（**Network Address Translator, NAT**）來增加私人網路位址，以解決 IP 位址不足的問題。

(B) IP 私有位址

IP 位址又分為『公共 IP』(Public IP)與『私有 IP』(Private IP) 兩種，在網路上通行的 IP 位址必須是屬於 Public IP 才行，Private IP 大多應用於私有網路內使用，不能通行於網際網路。在 A、B、C 這三個網路層級裡，個劃出一些位址範圍保留給私有位址使用，如下表：

網路層級	私有位址範圍
Class A	10.0.0.0 ~ 10.255.255.255
Class B	172.16.0.0 ~ 172.31.255.255
Class C	192.168.0.0 ~ 192.168.255.255

4-3-5 IP 封包結構

圖 5-10 為 IP 封包之資料結構，其中包含 IP 標頭和 IP 承載（IP Payload）（圖中 Data）兩大部份。IP 標頭的長度可以由 20 Bytes 到 60 Bytes 不等（由 IHL 欄位登錄），對整個 IP 封包長度可以是 46 ~ 1500 Bytes 之間（如圖 4-12 所示）。IP 標頭的各欄位功能如下：

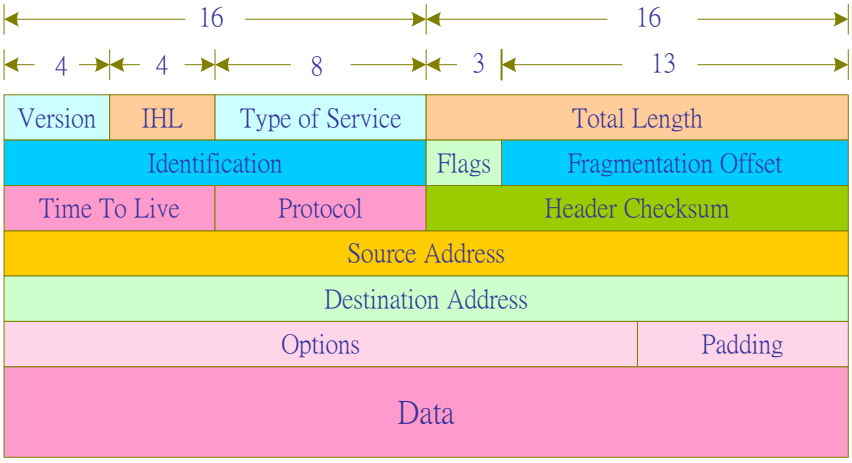


圖 4-12 IP 封包結構

- **版本（Version）：**4 位元。表示 IP 封包的 IP 版本。
- **網際標頭長度（Internet Header Length, IHL）：**4 位元。表示本 IP 封包標頭的長度（位元組表示）。範圍為 5 ~ 15，預設值為 5。
- **服務型態（Type of Service, TOS）：**8 位元。其內容為 "PPPDTRUU"，PPP 表示本 IP 封包的優先權(Precedence)；D = 0 表示一般延遲(Delay)，D = 1 表示低延遲；T = 0 為一般傳送量（Throughput），T = 1 為高傳送量；R = 0 為一般可靠度，R = 1 為高可靠度（Reliability）；UU 保留未用。
- **總長度（Total Length）：**16 位元。是指該封包的總長度，包括封包標頭及資料的長度，範圍由 576 ~ 65535 位元組。
- **辨識碼（Identification）：**8 位元。表示資料分割（fragmentation）的識別編號。同一筆資料如被分割成若干個區段，每段給予相同的辨識碼，接收端再依辨識碼組合回原來資料封包。
- **旗標（Flags）：**3 位元。其格式為 "0DM"。D = 0 表示可以分段，D = 1 為不可分段（Don’ t fragment）；M = 0 表示最後分段，M = 1 為不是最後分段（More fragment）。
- **分段偏移（Fragment Offset）：**13 位元。表示目前的分段在原始的資料中所在的位址。原始分段允許有 8192 個分段，以每 8 個位元為一個基本偏移量，所以最大容許 65536 位元資料，此值和總長度一樣。因此範圍為 0 ~ 8191，預設值為 0。

- **存活時間（Time to Live, TTL）：**8 位元。表示該封包在網路上的存活時間，封包每經過一個路由器（或網路閘門），該值就被減一。如路由器發現某封包的 TTL = 0，便將該資料片丟棄而不轉送。範圍 0 ~ 255。

- **協定號碼（Protocol Number）：**8 位元。表示該 IP 封包所承載通訊協定的協定號碼。在 TCP/IP 協定中，任何通訊協定（如 IP、ICMP、TCP、UDP 等等）的資料在傳送中都被包裝成 IP 封包，而以 IP 通訊協定發送。所以，在 IP 封包裡必須有協定號碼欄位，來表示目前所承載之資料是屬於哪一個通訊協定（IP、ICMP、TCP 等等）。一些較常用著名（well-known）的協定號碼如表 4-1 所示。

- **標頭檢查集（Header Checksum）：**16 位元。做標頭錯誤檢查用。

- **來源位址（Source Address）：**32 位元。發送此 IP 封包的來源位址。

- **目的位址（Destination Address）：**32 位元。目的主機之位址。

- **選項欄位（Options）：**可變長度。提供多種選擇性服務。目前已定義使用有下列：

  (1) 安全處理機制：有關資料加密與認證。

  (2) 路由紀錄：當 IP 封包經過路由器時，讓該路由器登錄其 IP 位址。當封包到達目的地時，可追蹤它所經過的路徑。

  (3) 時間戳記：當 IP 封包經過路由器時，讓路由器登錄其 IP 位址和時間。

  (4) 寬鬆來源路由（Loose Source Routing）：記錄該封包所必須經由之路徑，為一 IP 位址的序列表。

  (5) 嚴格來源路由（Strict Source Routing）：如同寬鬆來源路由，但嚴格規定祇能依照 IP 序列表傳送該封包。

- **填補欄位（Padding）：**IP 資料片的標頭一定是 32 位元的整數倍，當 Options 欄位不足 32 位元整數倍時由 Padding 欄位補足。

表 4-1 著名協定號碼（節錄）

協定名稱	協定號碼	協定全名（協定包裝在 IP 資料片內）

ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
GGP	3	Gateway-to –Gateway Protocol
IP	4	IP in IP encapsulation
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Protocol
UDP	17	User Datagram Protocol

4-3-6 IP 擷取與分析 - Wireshark

(A) 系統分析

在 TCP/IP 網路上除傳遞控制訊息(如 ARP、RARP、ICMP)外，應用服務大多使用 IP 封包傳送訊息，因此，只要隨便執行某一服務，即可擷取到 IP 封包。我們利用 chrome 瀏覽網頁就可以。

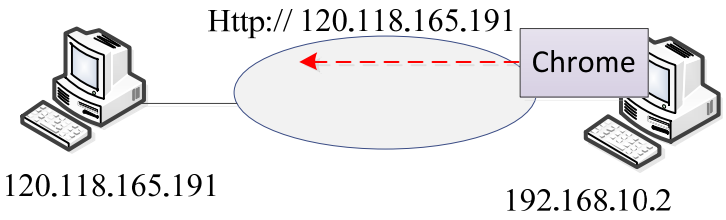


圖 4-13 擷取 IP 封包網路

(B) 擷取工具

我們需要用到下列工具：

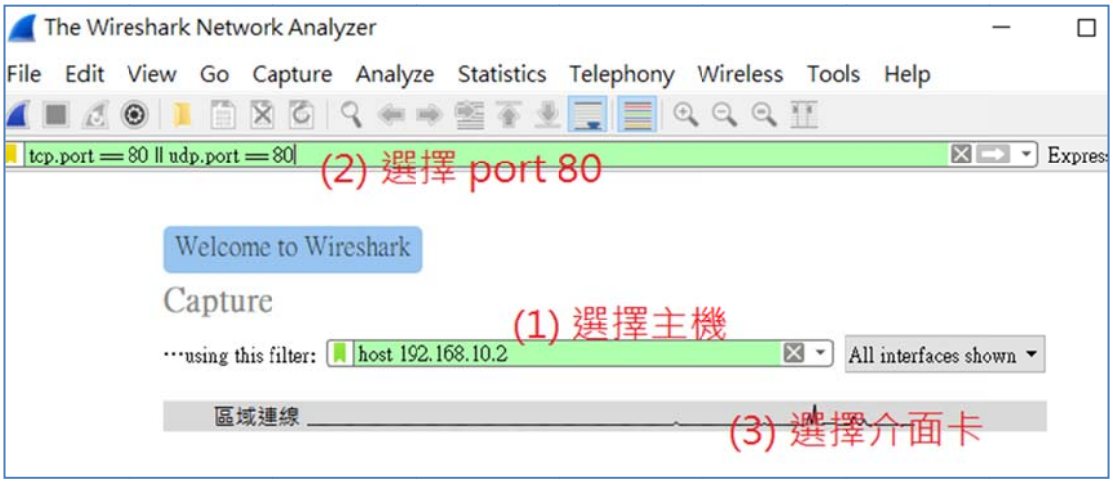
- Wireshark 網路封包分析器(安裝於 Windows 7)、
- 在 Windows 7/10 瀏覽器開啟某一個網站。

(C) 擷取封包步驟

(1) 開啟 Windows 命令提示字元，執行 ipconfig 命令，觀察工作站的 IP 位址。(如 192.168.10.2)

(2) 開啟 Wireshark

- 選擇擷取篩選條件：主機封包，如 192.168.10.2。
- 選擇顯示過濾條件：80/tcp、80/utp。
- 選擇擷取介面卡：區域網路連線。

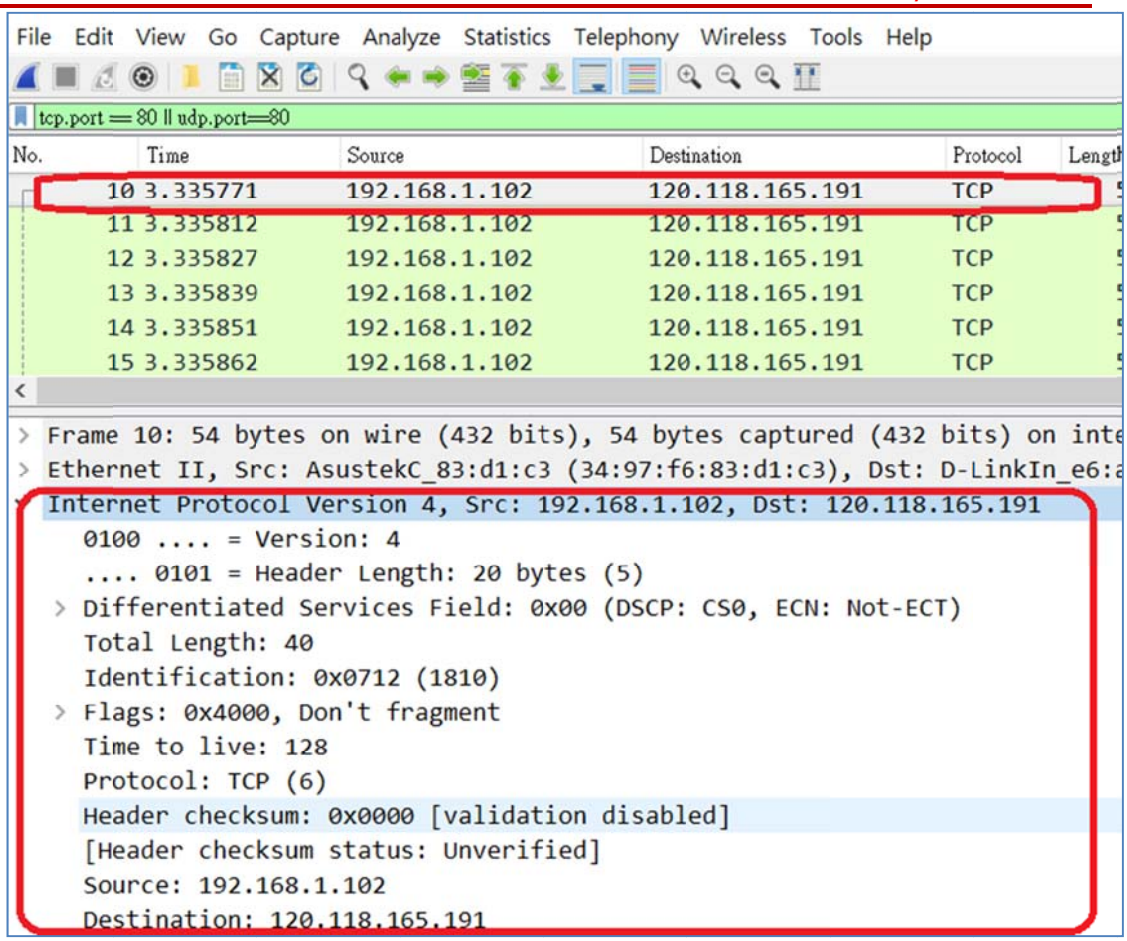


(3) 在 Windows 上聯覽某一網站(如 www.tsnien.idv.tw)

(4) 在 Wireshark 視窗按暫停，即可分析擷取到的。

(D) IP 協定分析

下圖為擷取到的封包，我們隨意分析某一封包即可。



吾人選擇某一筆 TCP 封包，再開啟『協定分析視窗』下的 IP 標頭分析，可以比較出各個欄位的內容，如下：

- Version：4
- IHL：0x0101
- Type of Service：0x00
- Total Length：20
- Identification：0x0712
- Flags：0x4000
- Fragmentation：Don't fragment
- Time to Live：128
- Protocol：TCP (6)
- Header Checksum：0x0000
- Source Address：192.168.1.102
- Destination Address：120.118.165.191
- Date：TCP Data

4-3-7 IP 擷取與分析 – Packet Tracer

(A) 系統分析

在 TCP/IP 網路上除傳遞控制訊息(如 ARP、RARP、ICMP)外，應用服務大多使用 IP 封包傳送訊息，因此，只要執行某一服務(Http 服務)，即可擷取到 IP 封包。

(B) 網路規劃

吾人利用 Packet Tracer 設計一個簡單網路，包含有三個 PC 電腦，期望網路環境如下：

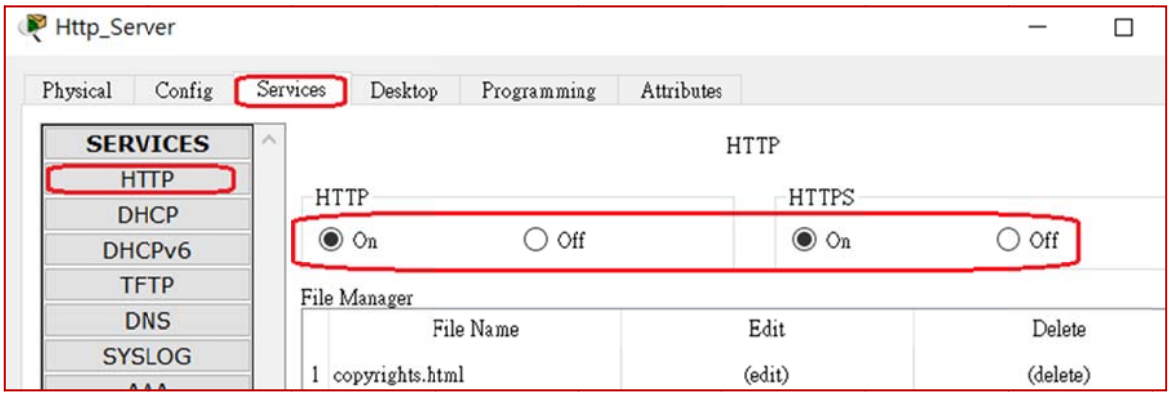
網路區段	Gateway/DNS	名稱	IP 位址	連接埠口
192.168.0.0/ 255.255.255.0	192.168.0.254/ 168.95.1.1	PC0	192.168.0.1	HUB(Fa0)
		PC1	192.168.0.2	HUB(Fa1)
		Http_Server	192.168.0.250	HUB(Fa5)

因此，我們需要在 Packet Tracer 上選擇下列裝置：

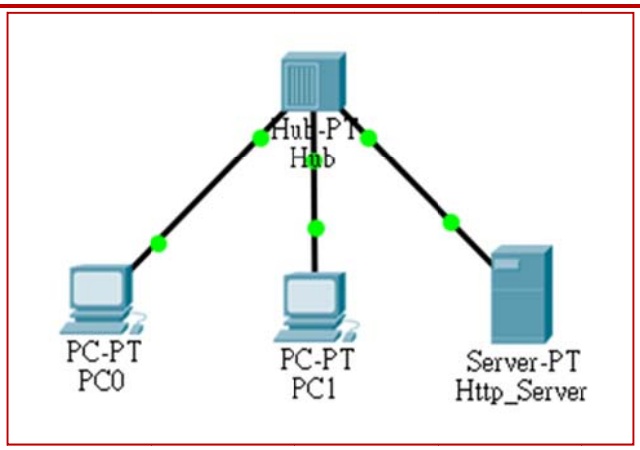
(1) Hub-PT：模擬集線器 (Hub) 一只。提供 PC 電腦之間連線。

(2) PC-PT：模擬 PC 主機二只。PC0 與 PC1 主機使用。

(3) Server-PT：模擬伺服器主機一只。開啟 HTTP Service，如下：



(4) 規劃網路如下：**(請下載 IP 封包擷取.pkt)**

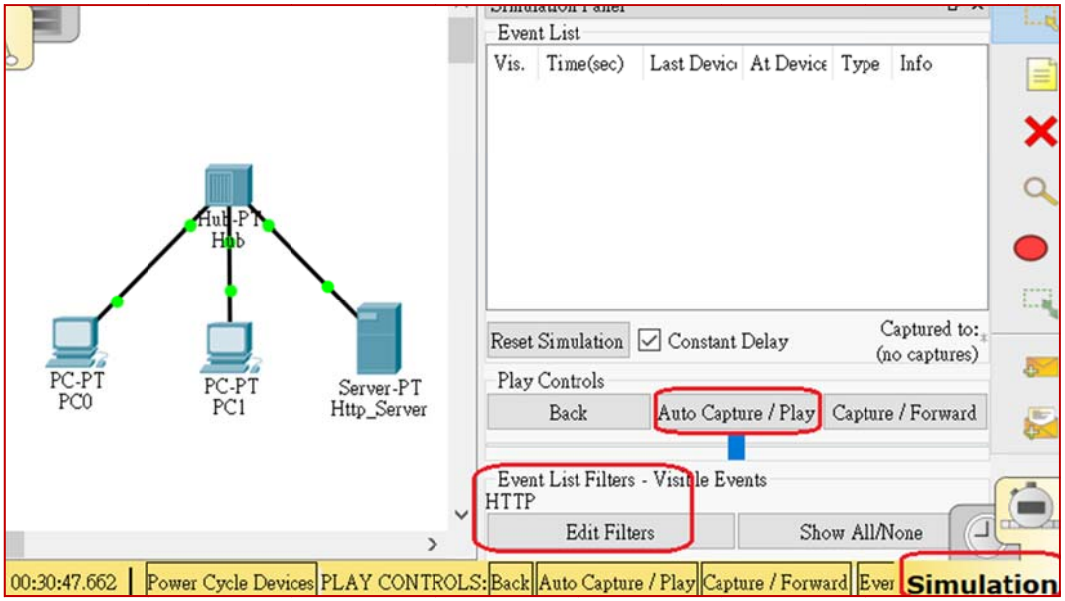


(C) 網路設定

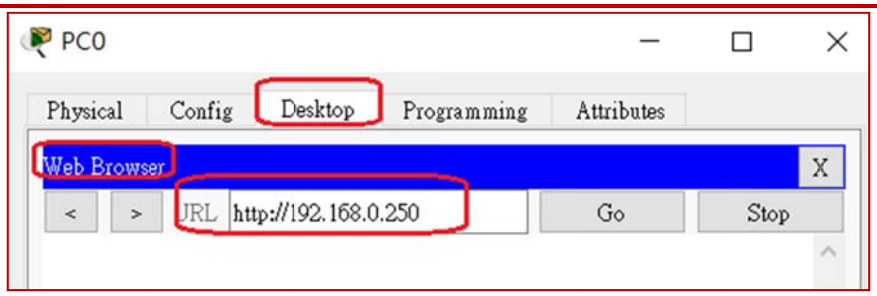
- 集線器 Hub 不需任何設定。
- PC0 與 PC2 須設定相關網路參數，如下(如 PC0)：Gateway = 192.168.0.254、DBS Server = 168.95.1.1、IP Address = 192.168.0.1、Subnet Mask = 255.255.255.0。
- Http_Service：Gateway = 192.168.0.254、DBS Server = 168.95.1.**1**、IP Address = 192.168.0.250、Subnet Mask = 255.255.255.0。

(D) 擷取封包步驟

(1) 步驟 1：Packet Tracer 採用 Simulation 模式，編輯 Edit Filters ，點選 HTTP，表示只擷取 HTTP 封包。



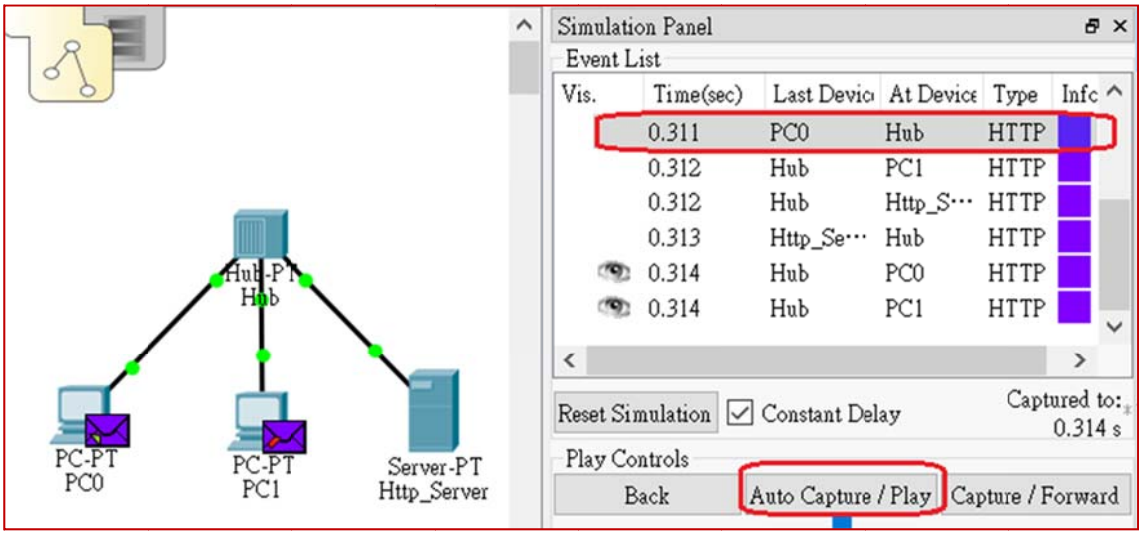
(2) 步驟 2：再由 PC0 上瀏覽 Web Server 如下：(點選 PC0 -> Desktop -> Web Browser ->)



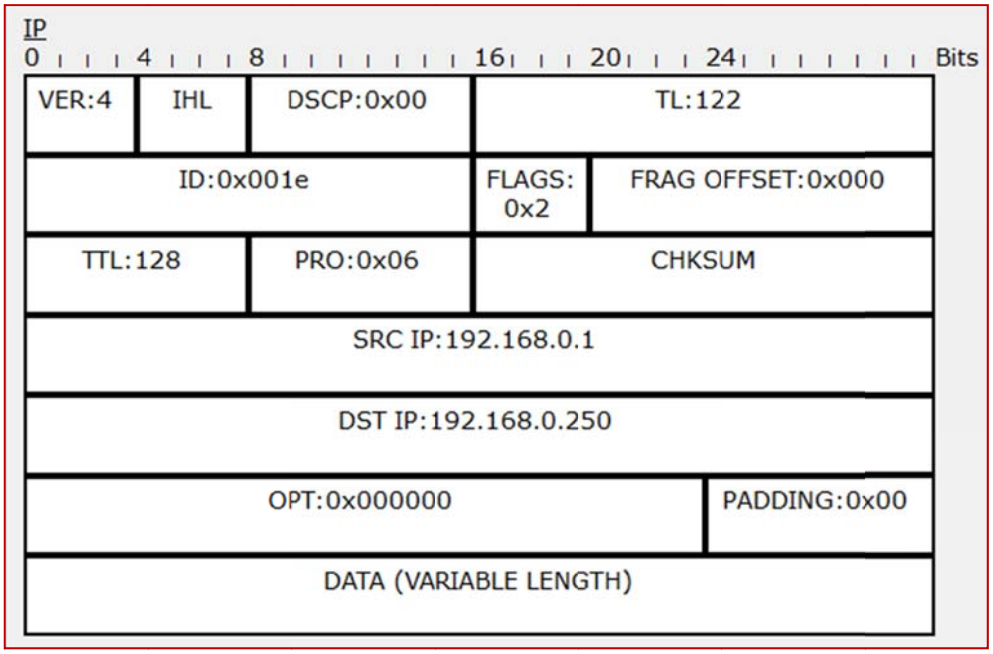
(3) 步驟 3：在 packet Tracer 上按『Auto Capture/Play』暫停。

(E) IP 協定分析

(1) 步驟 1：在 Packet Tracer 按『Auto Capture/Play』，則可觀察到擷取到 HTTP 的封包。



(2) 步驟 2：分析 IP 封包標頭，如下：



- TTL=128、PRO=0x06。
- SRC IP = 192.168.0.1。
- DST IP = 192.168.0.250。

4-4 ICMP 協定與分析

4-4-1 ICMP 協定功能

根據我們的瞭解 IP 網路是一種不可靠的傳輸方式，傳送中的封包必須經過多層路由器的轉送才能到達目的地，因此，在發送封包之前，我們很難預測該封包是否可以安全到達目的地。我們也很迫切地想知道目前網路的狀況，尤其在傳送失敗時，更想瞭解問題出在什麼地方。TCP/IP 網路中提供一種稱之為**『網際控制訊息協定』(Internet Control Message Protocol, ICMP)**的通訊軟體，用來偵測網路的狀況。在 IP 網路上，任何一部主機或路由器皆設置有 ICMP 協定，它們之間就可以利用 ICMP 來互相交換網路目前的狀況訊息，例如，主機不存在、網路斷線等等狀況。ICMP 訊息的產生有下列兩種情況：

(1) 障礙通知：當 IP 封包傳送當中，在某一網路上發生問題而無法繼續傳送，則會回應 ICMP 訊息給原封包傳送端。如圖 4-14 所示，訊號_1 是由 Router_A 回應；或是由 Router_B 回應訊號_2；也有可能是由主機 B 回應訊號_3。

(2) 狀況查詢：可以發送 ICMP 來查詢目前網路的情況。如圖 4-15 中，主機 A 發送 ICMP 查詢訊息，有可能由路由器回應 (訊號_1 和 訊號_2)，或由主機 B 回應訊號_3。

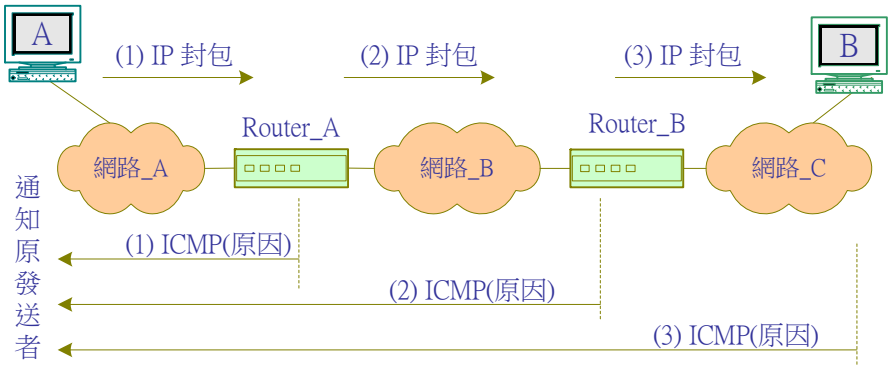


圖 4-14 ICMP 障礙通知

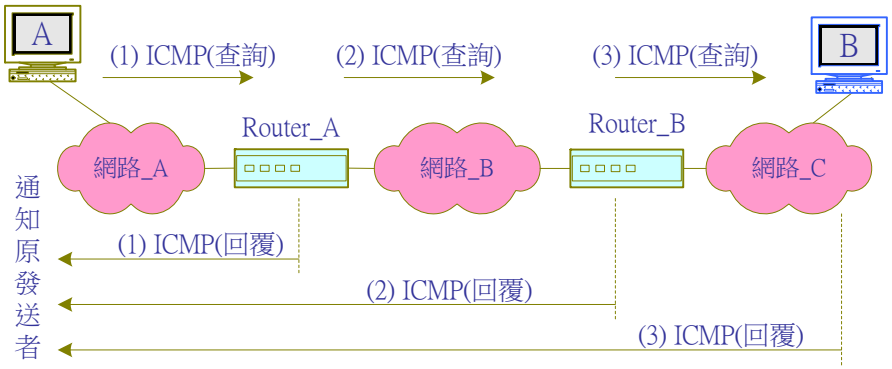


圖 4-15 ICMP 網路狀況查詢

4-4-2 ICMP 封包格式

ICMP 封包無法直接傳送到網路上，必須如同 TCP 封包一樣被嵌入 IP 封包內(如表 4-1)，以 IP 方式傳送，包裝在 IP 內的封包格式，如圖 4-16 所示。

圖 4-16 ICMP 封包嵌入 IP 封包內傳送

ICMP 封包的長度並不固定，隨著各種訊息型態而有不同的長度，圖 5-28 為 ICMP 封包格式，其各欄位功能如下：

- **訊息型態 (Message Type)**：表示該 ICMP 所欲控制之訊息型態，共有 13 種型態，訊息型態之型態代表值如表 4-2 所示。
- **編碼 (Code)**：對各種訊息型態進一步說明工作內容。
- **檢查集檢查碼 (Checksum)**：對該封包檢查集錯誤偵測。
- **訊息說明 (Message description)**：依照不同的控制訊息，而有不同的說明方式。
- **訊息資料 (Message Data)**：依照不同的控制訊息，而有不同的資料表示。

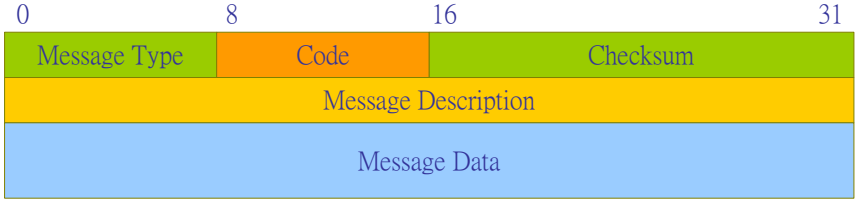


圖 4-17 ICMP 封包格式

表 4-2 ICMP 訊息型態

Message Type	ICMP 訊息功能
0	Echo Reply（回應答覆）
3	Destination Unreachable（目的地無法到達）
4	Source Quench（來源抑制）
5	Redirect（改變傳輸路徑）
8	Echo Request（回應要求）
9	Router Advertisement（路由器宣傳）
10	Router Solicitation（路由器懇請）
11	Time Exceeded for a Datagram（溢時傳輸）
12	Parameter Problem on a Datagram（參數問題）
13	Timestamp Request（時間標籤要求）
14	Timestamp Reply（時間標籤回覆）
15	Information Request（資訊要求）（停用）
16	Information Reply（資訊回覆）（停用）
17	Address Mask Request（位址遮罩要求）
18	Address Mask Reply（位址遮罩回覆）

4-4-3 ICMP 擷取與分析 - Wireshark

(A) 系統分析

ICMP 訊息封包有許多型態，我們以最常見的 Echo Request 與 Echo Reply 兩訊訊息來驗證，此兩訊息主要構成 Ping 命令。Ping 命令功能是測試網路連線是否正常，譬如，某主機執行 ping 192.168.1.1 命令，則由主機發送 ICMP Echo Request 給 192.168.1.1 主機，該主機如收到此封包，則會應 ICMP Echo Reply 訊息給發送者，如此連續測試若干次，如

果正常回應多次表示網路狀況良好；如果正常回應次數不多，則表示網路雖然可連線，但線路狀況不甚理想，必須尋找其他途徑解決問題；甚至都沒有回應，則表示網路不通。

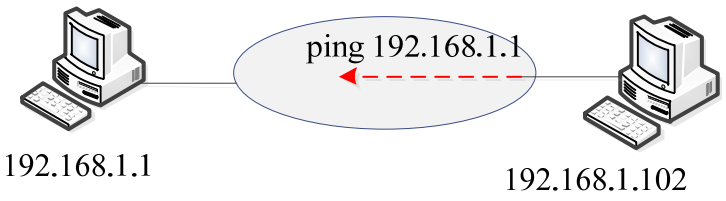


圖 4-18 擷取 ICMP 封包網路

我們利用 IP 封包標頭的 Protocol 欄位來辨識是否是 ICMP 封包，如 ip.pro = 0x01，則表示訊息內所乘載的 ICMP 封包。又利用 ICMP 標頭內的 Message Type 欄位來辨識訊息型態，如 MT=8 則是 Echo Request; MT=0 則是 Echo Reply。

(B) 擷取工具

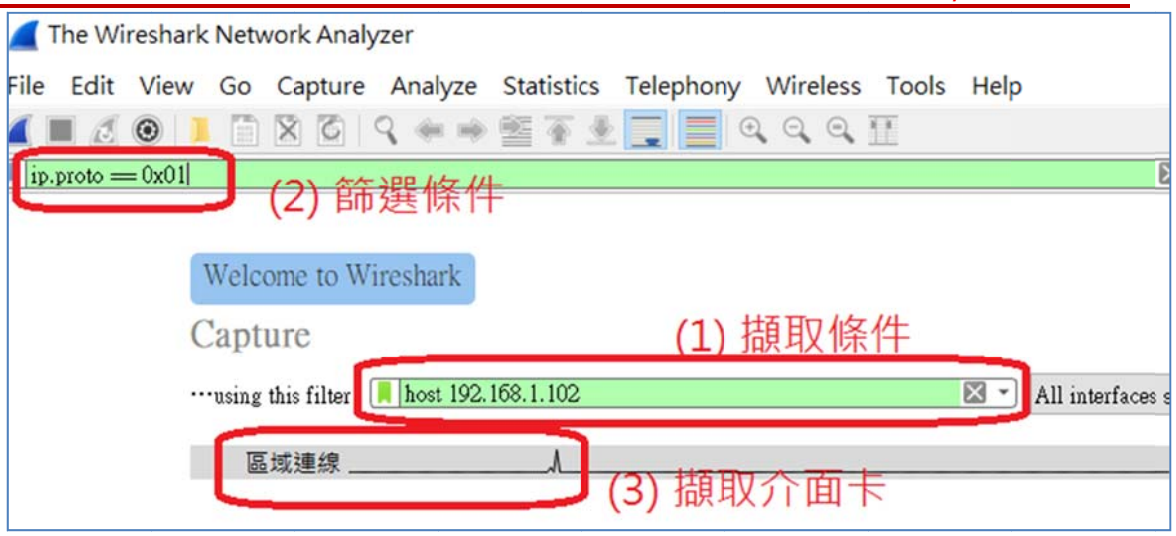
我們需要用到下列工具：

- Wireshark 網路封包分析器(安裝於 Windows 7)。
- Windows 命令提示字元(192.168.1.102)：執行 ping 192.168.1.1 命令。

(D) 擷取封包步驟

(1) 開啟 Wireshark：

- 擷取條件：host 192.168.1.102、
- 顯示篩選條件：ip.proto == 0x01(ICMP 封包)、
- 再選擇介面卡，如下：



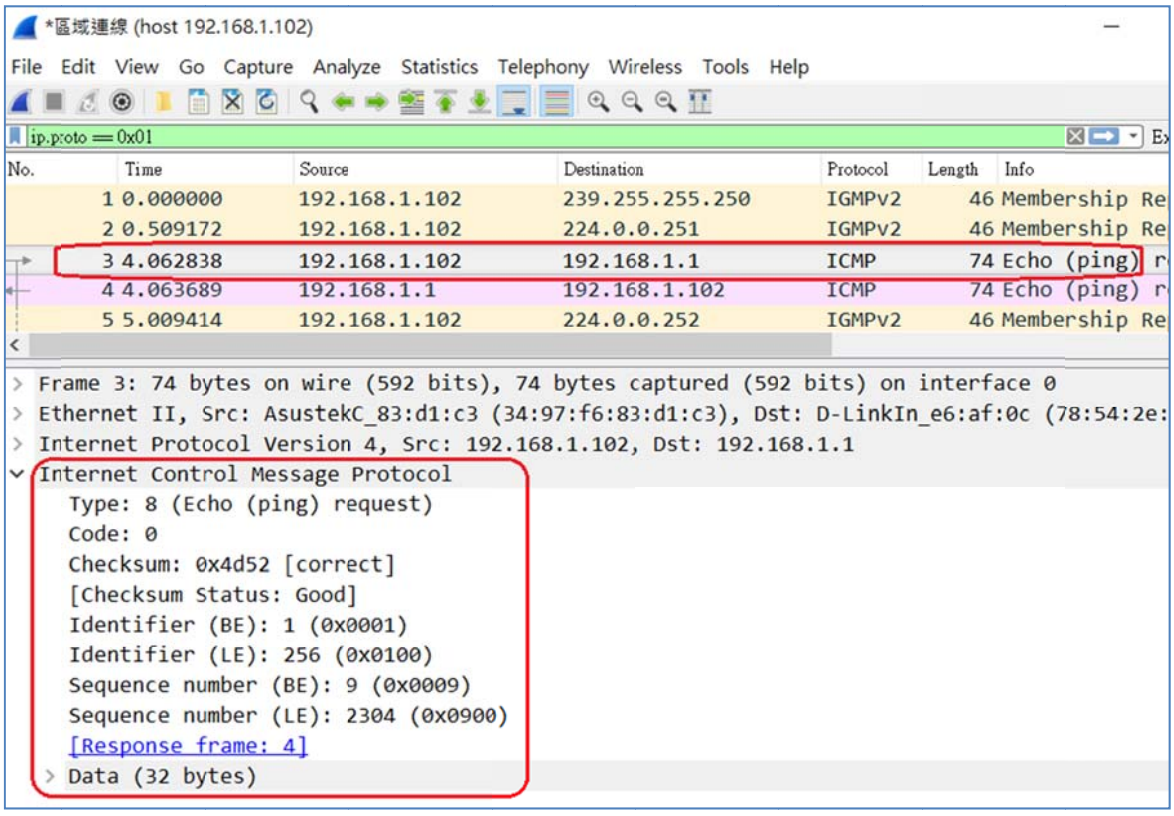
(2) 開啟 Windows 命令提示字元，執行 **> ping 192.168.1.1**

(3) 在 Wireshark 視窗按**暫停**。

(E) ICMP 協定分析

(E-1) Echo Request 封包分析

首先觀察 Echo request 封包格式 (序號 3)，由協定分析視窗比對出個欄位內容如下：



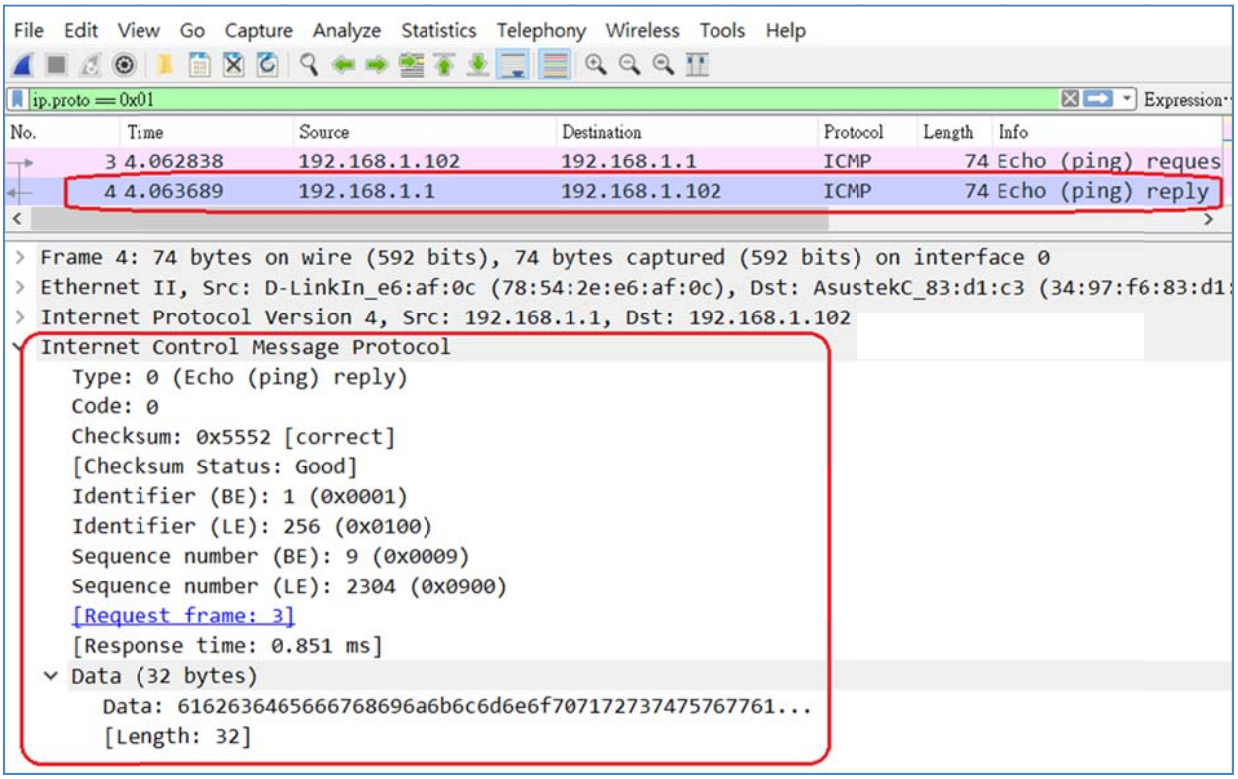
- Type：8 (Echo request)

- Code：0
- Checksum：0x4d52
- Identifier：(0x0001)(0x0009)
- Sequence number：(0x0009)(0x0900)

0	8	16	31
Type (0 或 8)	Code (0)	Checksum	
Identifier		Sequence Number	
Option Data			

(E-2) Echo reply 封包

Echo reply(序號 4) 封包分析如下：



- Type：0 (Echo reply)
- Code：0
- Checksum：0x5552

4-4-4 ICMP 擷取與分析 – Packet Tracer

(A) 系統分析

ICMP 訊息封包有許多型態，我們以最常見的 Echo Request 與 Echo Reply 兩訊訊息來驗證，此兩訊息主要構成 Ping 命令。Ping 命令功能是測試網路連線是否正常，譬如，某主機執行 ping 192.168.1.1 命令，則由主機發送 ICMP Echo Request 給 192.168.1.1 主機，該主機如收到此封包，則會應 ICMP Echo Reply 訊息給發送者，如此連續測試若干次，如果正常回應多次表示網路狀況良好；如果正常回應次數不多，則表示網路雖然可連線，但線路狀況不甚理想，必須尋找其他途徑解決問題；甚至都沒有回應，則表示網路不通。

我們利用 IP 封包標頭的 Protocol 欄位來辨識是否是 ICMP 封包，如 ip.pro = 0x01，則表示訊息內所乘載的 ICMP 封包。又利用 ICMP 標頭內的 Message Type 欄位來辨識訊息型態，如 MT=8 則是 Echo Request; MT=0 則是 Echo Reply。

(B) 網路規劃

吾人利用 Packet Tracer 設計一個簡單網路，包含有三個 PC 電腦，期望網路環境如下：

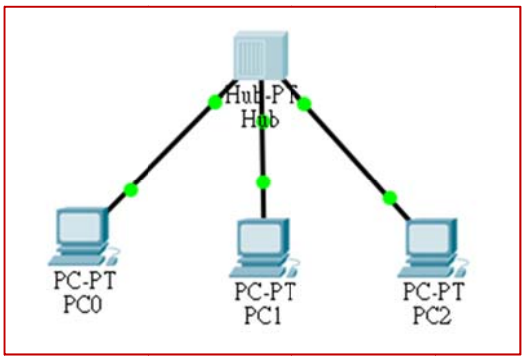
網路區段	Gateway/DNS	名稱	IP 位址	連接埠口
192.168.0.0/ 255.255.255.0	192.168.0.254/ 168.95.1.1	PC0	192.168.0.1	HUB(Fa0)
		PC1	192.168.0.2	HUB(Fa1)
		PC2	192.168.0.3	HUB(Fa2)

因此，我們需要在 Packet Tracer 上選擇下列裝置：

(1) Hub-PT：模擬集線器 (Hub) 一只。提供 PC 電腦之間連線。

(2) PC-PT：模擬 PC 主機三只。PC0 ~ PC2 主機使用。

(3) 規劃網路如下：**(請下載 ICMP 封包擷取.pkt)**



(C) 網路設定

- 集線器 Hub 不需任何設定。
- PC0 ~ PC3 須設定相關網路參數，如下(如 PC0)：Gateway = 192.168.0.254、DBS Server = 168.95.1.1、IP Address = 192.168.0.1、Subnet Mask = 255.255.255.0。

(D) 擷取封包步驟

(1) 步驟 1：Packet Tracer 採用 Simulation 模式，編輯 Edit Filters ，點選 ICMP，表示只擷取 ICMP 封包。

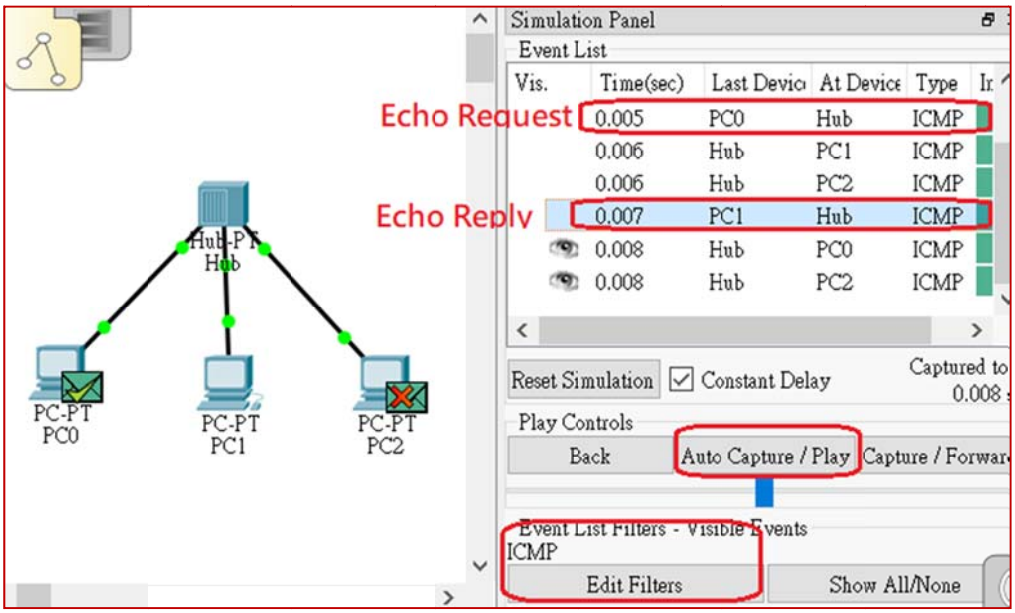
(2) 步驟 2：再由 PC0 上 ping 發送給 PC0 如下：(點選 PC0 -> Desktop -> Command Prompt ->)

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
```

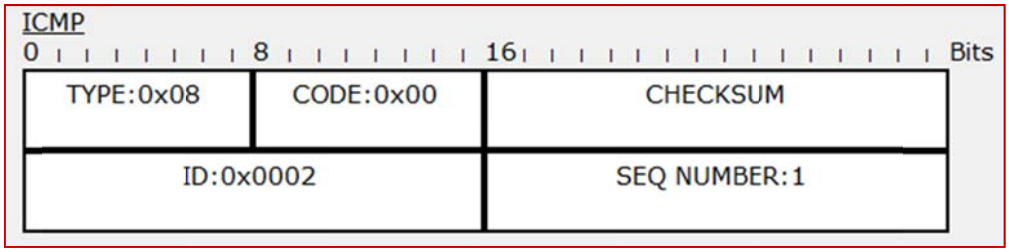
(3) 步驟 3：在 packet Tracer 上按『Auto Capture/Play』暫停。

(E) ICMP 協定分析

(1) 步驟 1：在 Packet Tracer 按 『Auto Capture/Play』，則可觀察到擷取到 ARP 的封包，其中包含 Echo Request 與 Echo Reply 兩封包。

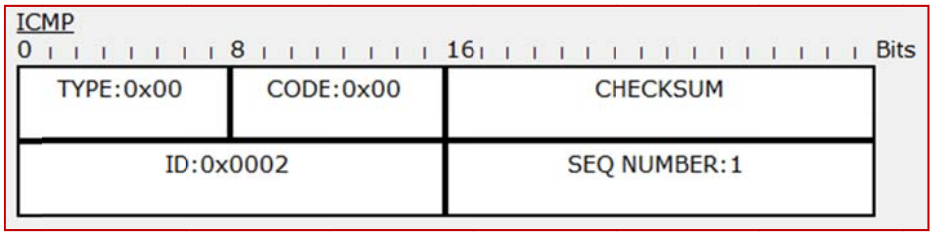


(2) 步驟 2：分析 Echo Request 封包標頭，如下：



- Type = 0x08 (Echo Request)、
- Code = 0x00、ID = 0x0002、Seq = 1。

(3) 步驟 3：分析 Echo Reply 封包標頭，如下：



- Type = 0x00 (Echo Reply)、
- Code = 0x00、ID = 0x0002、Seq = 1。

4-5 TCP 協定與分析

4-5-1 TCP 協定功能

『傳輸控制協定』(Transmission Control Protocol, TCP)和 IP 兩者似乎是連結在一起的同一名稱 (TCP/IP)，兩者的功能確實是相輔相成。IP 的功能是無論兩部工作站在無遠弗屆的任一個角落，都能將它們連結在一起。TCP 提供網路的服務接點讓應用程式使用，也就是說，提供端點對端點 (End-to-End) 的連線。主機電腦上有多個應用程式都必須透過網路提供或使用網路服務，TCP 就提供多點服務的連線 (虛擬鏈路的多工功能) 讓各種應用程式可同時連結到網路上。TCP 和 IP 的關係宛如電話系統中的電話號碼和分機號碼。當我們撥接電話時，將依照電話號碼的位址在廣泛的電話大海之中找到對方，並和其連接完成 (IP 功能，各地區的交換機就如網路閘門)。這並不能表示我們已連絡上受話的對方，但最起碼我們也連線到對方的電話機上 (IP 已連結到主機上)。欲找到受話的人也許可用人工呼叫，但也

可以再撥分機號碼（TCP 的埠口號碼），這表示在主機號碼上再加入分機號碼來表示通訊的個人（TCP 的點對點連線）。人與人之間的對話就像網路上應用程式之間的通訊。

TCP 和 IP 另一個相輔相成的功能是 IP 提供非連接的不可靠傳輸，對於有關可靠傳輸的處理程序就必須仰賴 TCP 來完成。換言之，IP 傳送當中，也許會發生封包損壞、封包遺失、封包重複或次序錯亂等現象，這些情況都必須由 TCP 來負責檢測出，並要求對方重送、重整封包順序等工作。因此，TCP 必須提供連接導向的連線，才能使整個網路通訊達到可靠性的傳輸。重點說明如下：

- 端點對端點連線 (End-to-End Connection)
- 提供服務連接埠口(Port)：

  (1) 0 ~ 1023：著名埠口，如 80/tcp 連接 http Server。

  (2) 1024 ~ 65535：使用者或動態埠口。
- 連接導向方式

  (1) 虛擬連線建立。

  (2) 檢視錯誤與遺失封包。

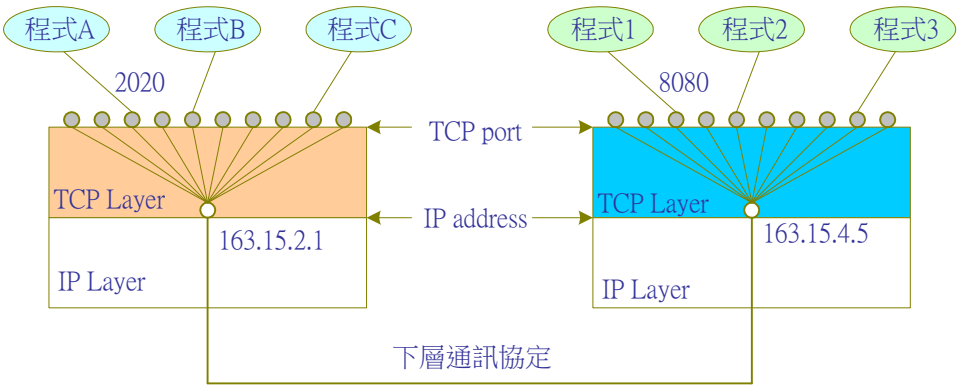


圖 4-19 TCP 通訊連線

4-5-2 TCP 封包格式

傳輸層的 TCP/UDP 封包經過 IP 封包包裝，又再經過 Ethernet 訊框包裝後，才發送到網路上，其包裝結構如圖 4-20 所示。

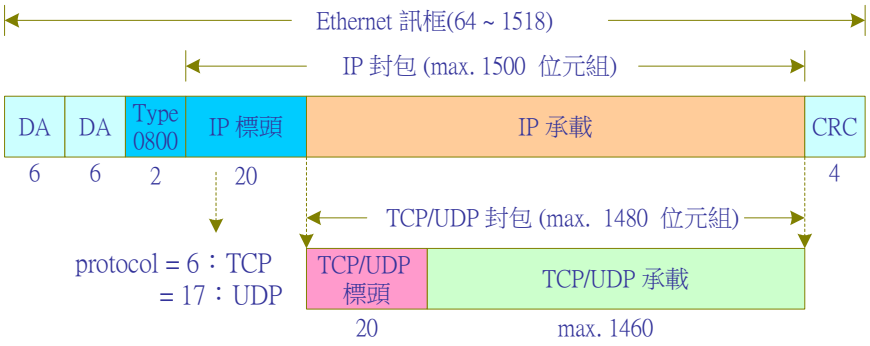


圖 4-20 Ethernet 訊框包裝

在 Ethernet 框標頭中，型態（Type）為 0x0800 表示該訊框是承載 IP 封包，又在 IP 封包標頭中，如 Protocol 欄位為 6 表示本封包是承載 TCP 訊息；如 Protocol = 17 則表示承載 UDP 訊息。一般傳送 TCP/IP 訊息，IP 標頭大多不會攜帶特殊訊息（如來源路徑選擇），也沒有選項欄位（Option），因此 IP 標頭佔用 20 位元組長度。TCP 標頭如沒有特殊訊息，也是佔用 20 位元組長度。而一般 UDP 標頭也都是佔用 20 位元組。如下：

- Eth.type = 0x0800
- Ip.pro = x06

圖 4-21 為 TCP 的封包格式，各欄位功能如下：

- **來源埠口（Source Port）：**來源之 TCP 埠口。
- **目的地埠口（Destination Port）：**目的地之 TCP 埠口。
- **順序編號（Sequence Number）：**該封包的順序編號。
- **確認號碼（Acknowledge Number）：**回應封包的確認號碼，也是期望傳送端下次發送封包的序號，其表示該確認號碼以前的封包都以正常接收。
- **資料偏移量（Data Offset）：**因為 TCP 的 Option 欄位長度並非固定，Data Offset 用來表示傳輸資料（Data）是在整個封包之區段起始位址。
- **位元碼（Code bits）：**（6 位元）（URG, ACK, PSH, TST, SYN, FIN）此欄位作控制訊息傳遞之用。而且目前有關 TCP/IP 網路上的特殊處理工作（如防火牆等等）都是利用這些控制碼來運作。其中：

(1) URG（Urgent）：表示該封包為緊急資料，並使 Urgent Point 欄位有效。

(2) ACK（Acknowledge）：本封包有回應確認功能，其確認 Acknowledge Number 欄位中所指定的順序號碼。

(3) PSH（Push）：請求對方立即傳送 Send Buffer 中的封包。

(4) RST（Reset）：要求對方立即結束連線（強迫性），且發送者已斷線。

(5) SYN（Synchronous）：通知對方要求建立連線（TCP 連線）。

(6) FIN（Finish）：通知對方，資料已傳輸完畢，是否同意斷線。發送者還在連線中等待對方回應。

- **視窗（Window）：**此欄位是用來控制封包流量，告訴對方目前本身還有多少緩衝器（Receive Buffer）可以接收封包（滑動視窗法之特性）。如果 Window = 0 表示緩衝器已滿暫停傳送資料。Window 大小的單位是以位元組表示（Byte）。
- **檢查集（Checksum）：**此欄位為 16 bits 長的檢查碼，接收方可依此 Checksum 來確定所收封包（資料極表頭）是否正確。
- **緊急指標（Urgent Point）：**當 URG = 1 時，其代表緊急資料是在資料區的什麼位址。
- **任選欄（Option）：**目前此欄位只應用於表示接收端能夠接收最大資料區段的大小。如果不使用此欄位，則可以使用任意的資料區段大小。
- **填補欄位（Padding）：**將 Option 欄位補足 32 位元的整數倍。

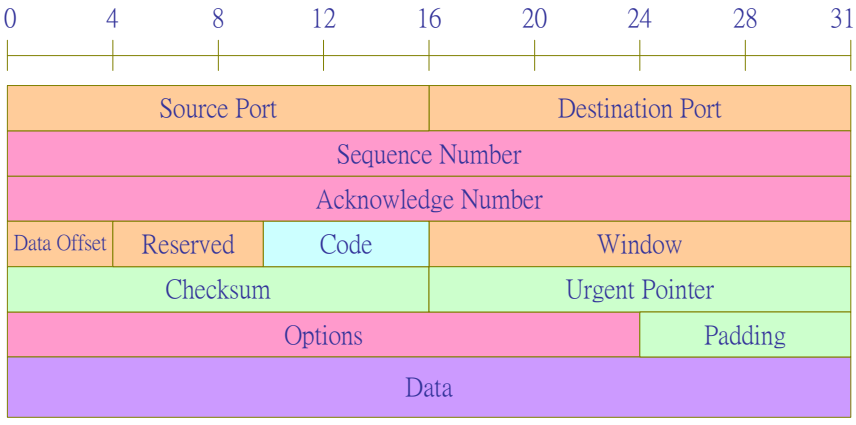


圖 4-21 TCP 封包格式

4-5-3 TCP 建立連線

Tomlinson（1975）提出三向式握手法（Three-way handshake）。其運作的主要原理，就是不管要求訊號或回應訊號都編有序號，尤其回應時必須指明這是回應第幾號要求連線訊息。對於序號的編列不必依照一定的順序，只要能標示出獨立訊息便可以。如圖 4-22 所示，工作站 A（TP_A）送出要求連接訊號（Connect Request，CR）並附帶序列號碼 x（seq=x）；工作站 B（TP_B） 針對 TP_A 的要求而送出同意連線訊號 （Ack(ack=x)），並標示出本回應訊號的序號（seq=y）；TP_A 接到 TP_B 的同意連線訊號 Ack（seq=y, ack=x），便知道是針對哪一個連線要求的回應，並在傳送一個確認訊號表示連線成功 Ack(seq=x, ack=y); TP_B 收到確認訊號也知道針對哪一個連線已連接成功。

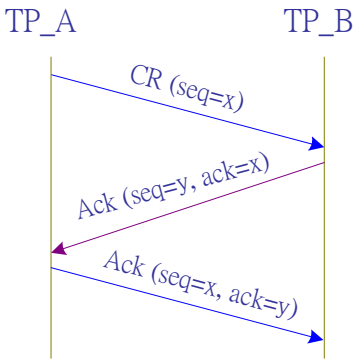


圖 4-22 三向握手式連絡法之訊號方式

因此，TCP 採用三向握手式連絡法（Three-way handshake）來實現連線處理，其中會用到封包內二個序號：Sequence Number（seq）及 Acknowledge Number（ack），以及 Code（或稱 Flags）欄位中四個旗標：ACK、SYN、FIN 和 RST。有三個訊號來建立連線，如下：

(1) 發起者要求連線： 發起者發送 TCP 封包，標頭內 SYN = 1，表示要求連線；

(2) 回應者同意連線：回應者如同意連線，則回送 TCP 封包，標頭內 SYN = 1 & ACK = 1，表示同意連線要求；

(3) 發起者確認連線：發起者收到同意連線訊息後，最後確認連線成功則回應 ACK =1。

另外，針對上述對話連線，有可能連線經過網路延誤而重新發送訊息，為了確認是針對哪一個對話連線回應，則以 seq = 連線號碼，來表示哪一對話，回應時 ack = seq +1，表示針對

哪一個連線號碼回應，並要求傳遞下一個封包序號（滑動視窗法確認方式，詳情請參閱 **TCP/IP 與 Internet 網路**）。

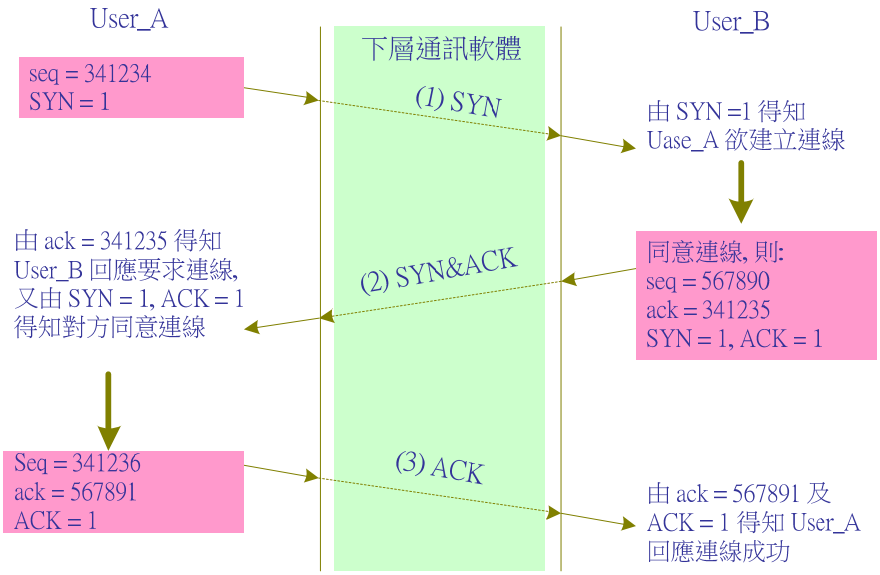


圖 4-23 TCP 建立連線運作程序

4-5-4 TCP 擷取與分析 - Wireshark

(A) 系統分析

欲擷取 TCP 連線封包很容易，網路應用系統大多採用 TCP 協定，吾人在 Windows 上瀏覽某一網站(www.tsnien.idv.tw)，再擷取 httpd 封包即可。

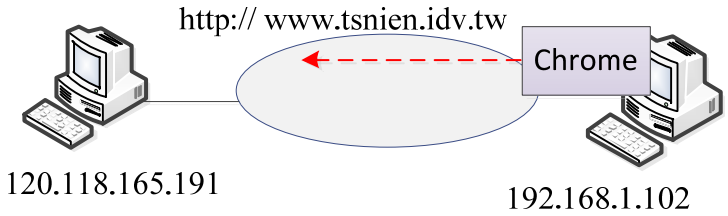


圖 4-24 TCP 封包擷取網路

(B) 擷取工具

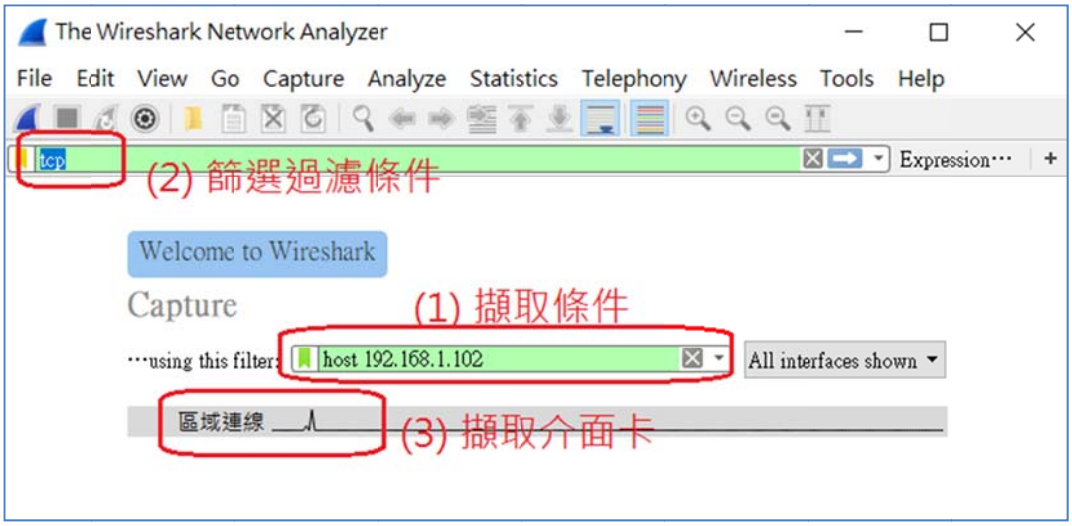
此實習題目，需要用到下列工具：

- Wireshark 網路封包分析器(安裝於 Windows 7)
- Windows 上瀏覽 www.tsnien.idv.tw 網頁。

(C) 擷取封包步驟

(1) 開啟 Wireshark：

- 擷取條件：host 192.168.1.102 (windows IP)、
- 顯示篩選條件：tcp、
- 再選擇介面卡，如下：



(2) Windows 上瀏覽 www.tsnien.idv.tw 網頁。

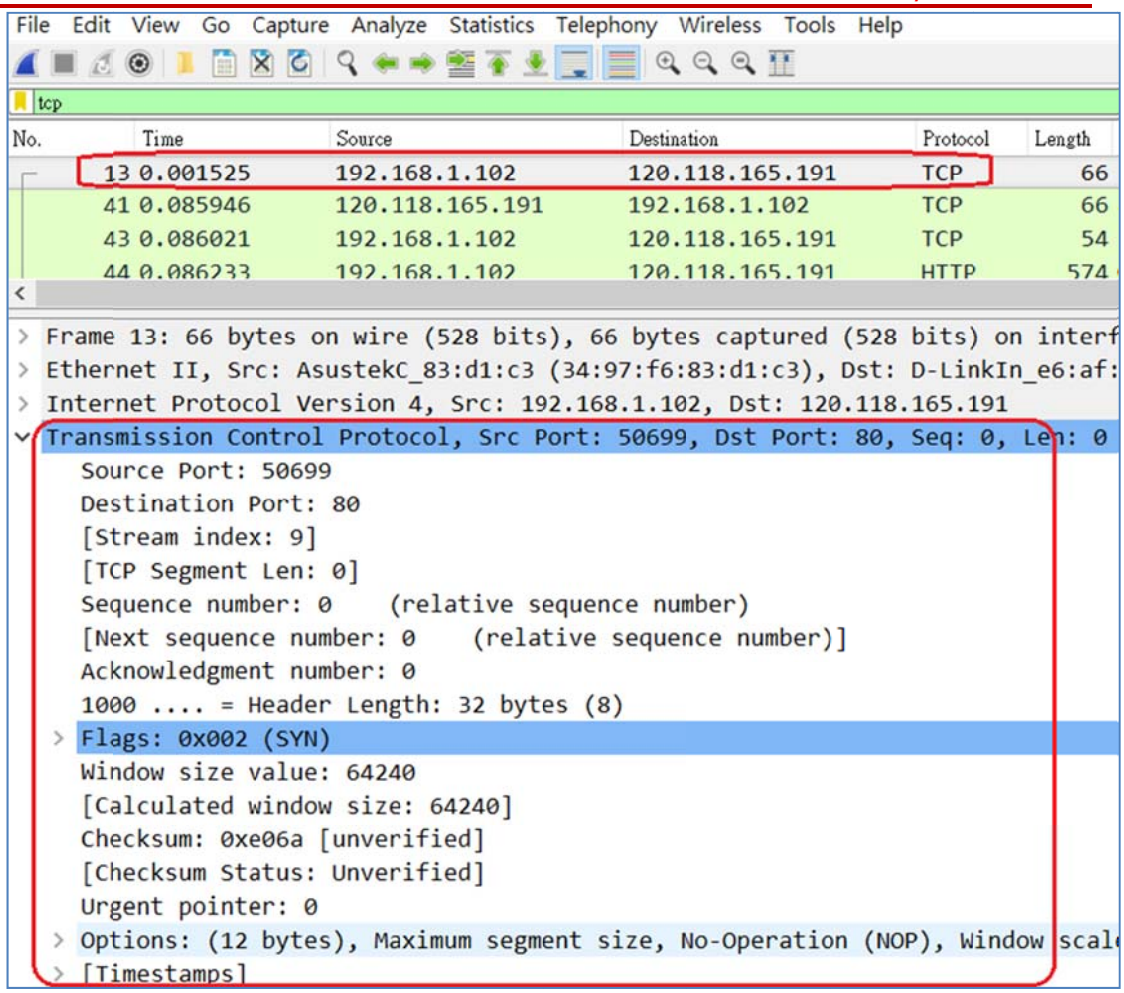
(3) 在 Wireshark 視窗按暫停。

(D) TCP 協定分析

(D-1) 客戶端建立連線封包

由上圖中第 13 封包是客戶端要求建立連線的封包。各欄位分析如下：(僅說明重要欄位，其他請自行比較參考)

- IP 封包標頭，如下：
  - Source：192.168.1.102
  - Destination：120.118.165.191 (www.tsnien.idv.tw)
  - Protocol：TCP



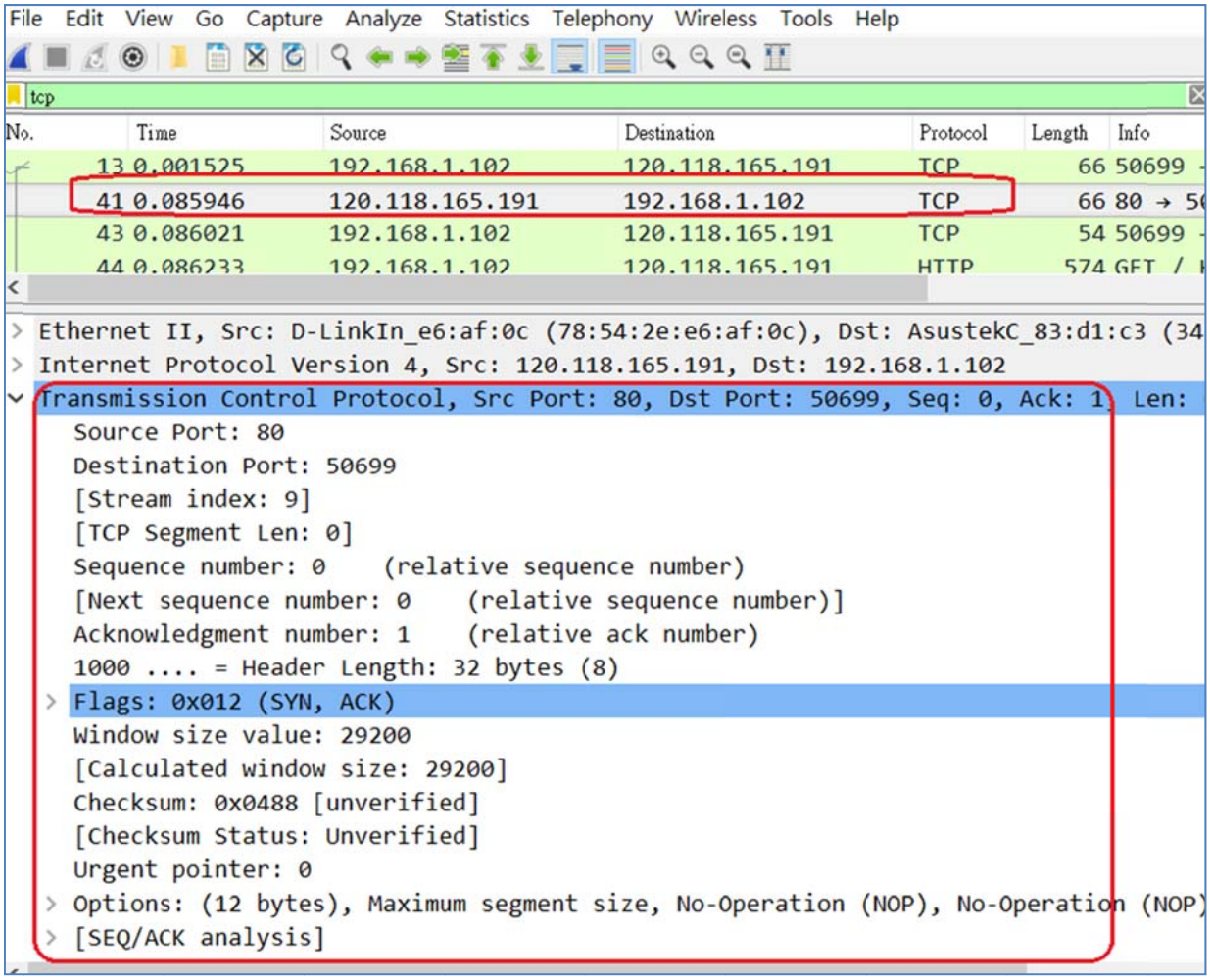
- TCP 封包標頭，如下：
  - Source Port：50699
  - Destination Port：80
  - Sequence Number：0
  - Acknowledge Number：0
  - Flags：0x002 (SYN)(客戶端要求連線)
  - Window size value0：64240

(D-2) 伺服端回應同意連線封包：

第 41 封包是伺服端同意連線的封包。各欄位分析如下：(僅說明重要欄位，其他請自行比較參考)

- IP 封包標頭，如下：
  - Source：120.118.165.191 (www.tsnien.idv.tw)
  - Destination：192.168.1.102

- Protocol：TCP



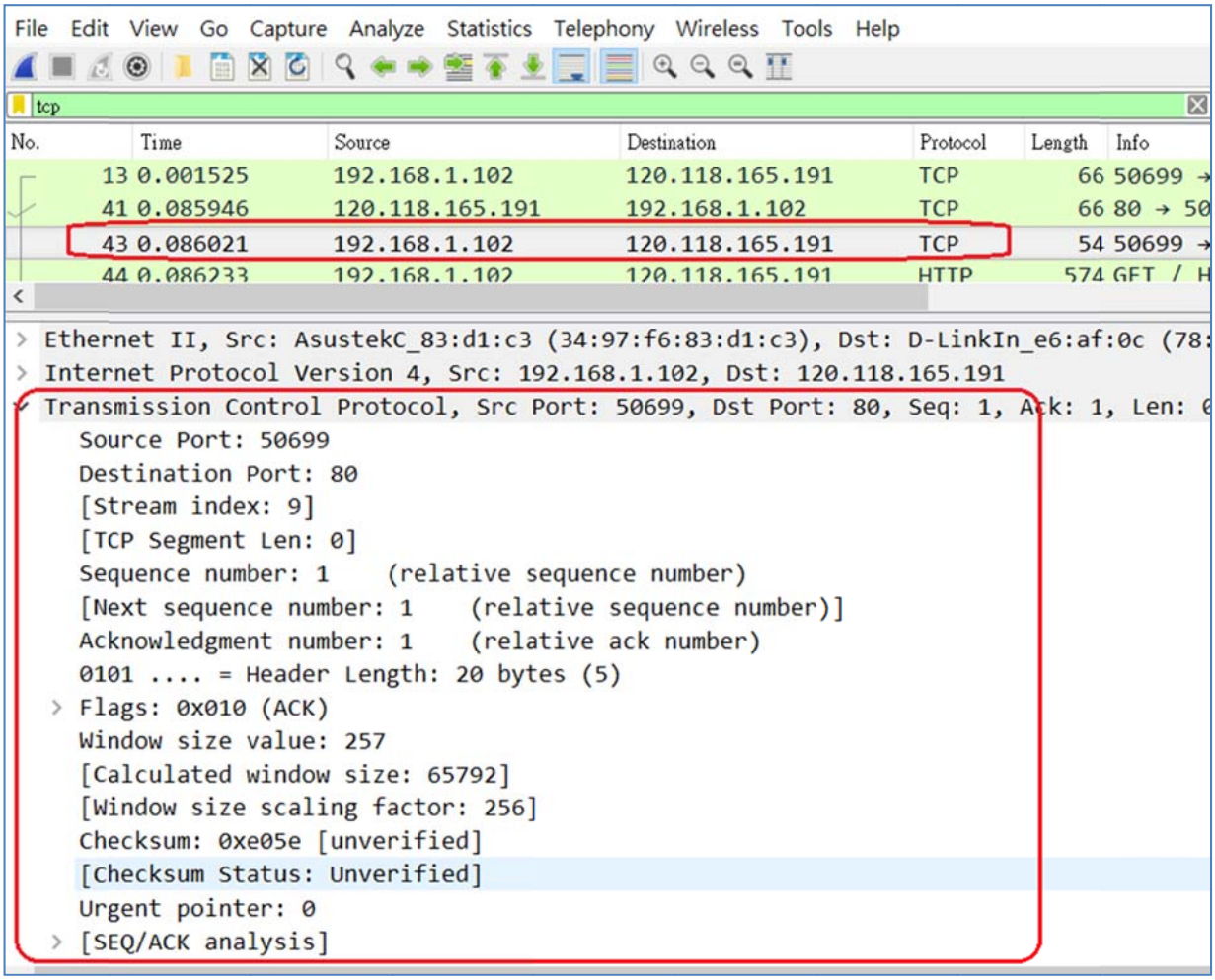
- TCP 封包標頭，如下：
  - Source Port：80
  - Destination Port：50699
  - Sequence Number：0
  - Acknowledge Number：1
  - Flags：0x012 (SYN, ACK)(伺服端同意連線)

(D-3) 客戶端確認連線成功：

第 43 封包是客戶端確認連線成功。各欄位分析如下：(僅說明重要欄位，其他請自行比較參考)

- IP 封包標頭，如下：
  - Source：192.168.1.102

- Destination：120.118.165.191 (www.tsnien.idv.tw)
- Protocol：TCP



TCP 封包標頭，如下：

- Source Port：50699
- Destination Port：80
- Sequence Number：1
- Acknowledge Number：1
- Flags：0x010 (ACK)(客戶端確認連線成功)

4-5-5 TCP 擷取與分析 – Packet Tracer

(A) 系統分析

欲擷取 TCP 連線封包很容易，網路應用系統大多採用 TCP 協定，吾人在 PC 瀏覽某一網站，再擷取 httpd 封包即可。

(B) 網路規劃

吾人利用 Packet Tracer 設計一個簡單網路，包含有三個 PC 電腦，期望網路環境如下：

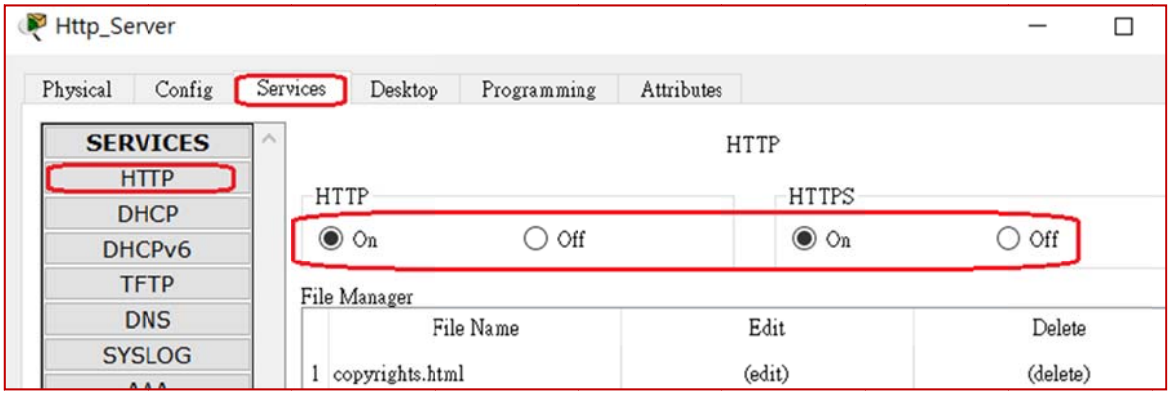
網路區段	Gateway/DNS	名稱	IP 位址	連接埠口
192.168.0.0/ 255.255.255.0	192.168.0.254/ 168.95.1.1	PC0	192.168.0.1	HUB(Fa0)
		Http_Server	192.168.0.250	HUB(Fa5)

因此，我們需要在 Packet Tracer 上選擇下列裝置：

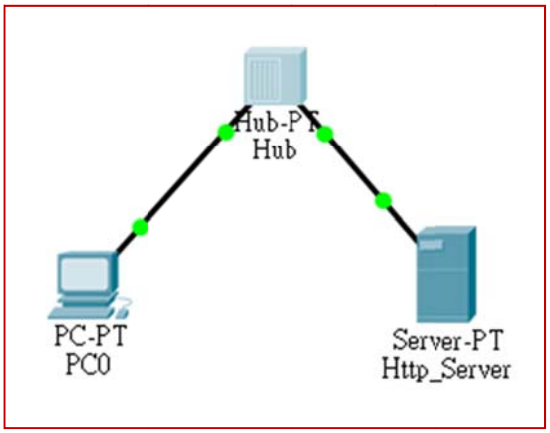
(1) Hub-PT：模擬集線器 (Hub) 一只。提供 PC 電腦之間連線。

(2) PC-PT：模擬 PC 主機一只。PC0 主機使用。

(3) Server-PT：模擬伺服器主機一只。開啟 HTTP Service，如下：



(4) 規劃網路如下：**(請下載 TCP 封包擷取.pkt)**



(C) 網路設定

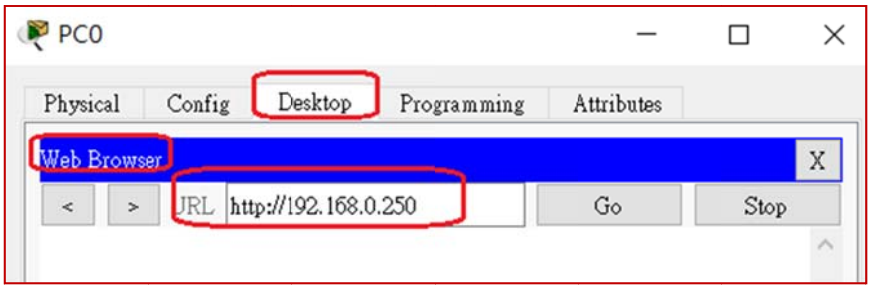
- 集線器 Hub 不需任何設定。

- PC0 與 PC2 須設定相關網路參數，如下(如 PC0)：Gateway = 192.168.0.254、DBS Server = 168.95.1.1、IP Address = 192.168.0.1、Subnet Mask = 255.255.255.0。
- Http_Service：Gateway = 192.168.0.254、DBS Server = 168.95.1.**1**、IP Address = 192.168.0.250、Subnet Mask = 255.255.255.0。

(D) 擷取封包步驟

(1) 步驟 1：Packet Tracer 採用 Simulation 模式，編輯 Edit Filters ，點選 TCP，表示只擷取 TCP 封包。

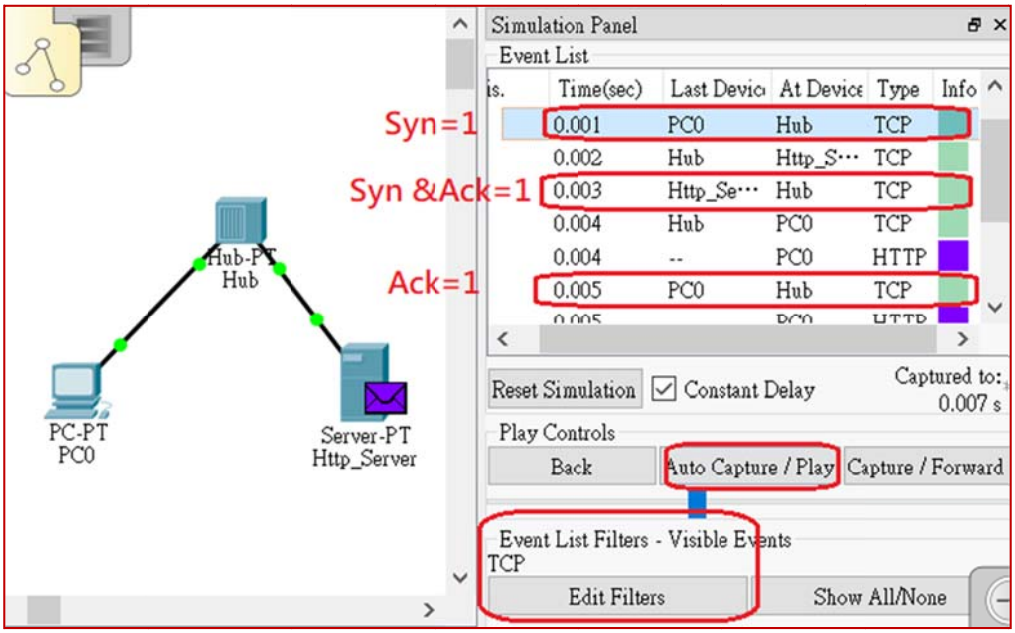
(2) 步驟 2：再由 PC0 上瀏覽 Http_Server 網頁：(點選 PC0 -> Desktop -> Web Browser)



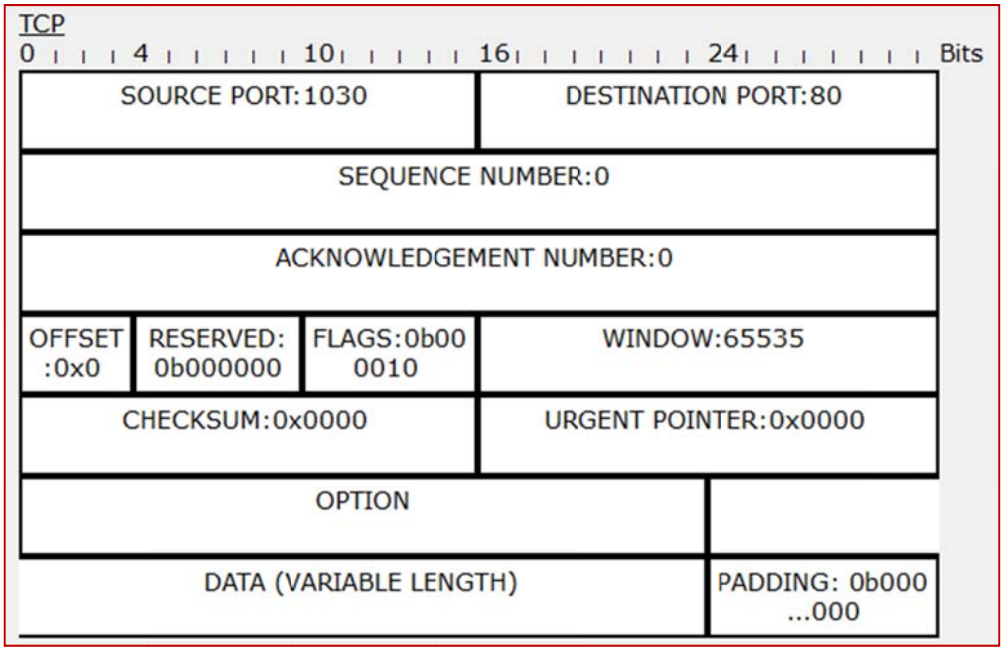
(3) 步驟 3：在 packet Tracer 上按『Auto Capture/Play』暫停。

(E) TCP 協定分析

(1) 步驟 1：在 Packet Tracer 按 『Auto Capture/Play』，則可觀察到擷取到 TCP 的封包。

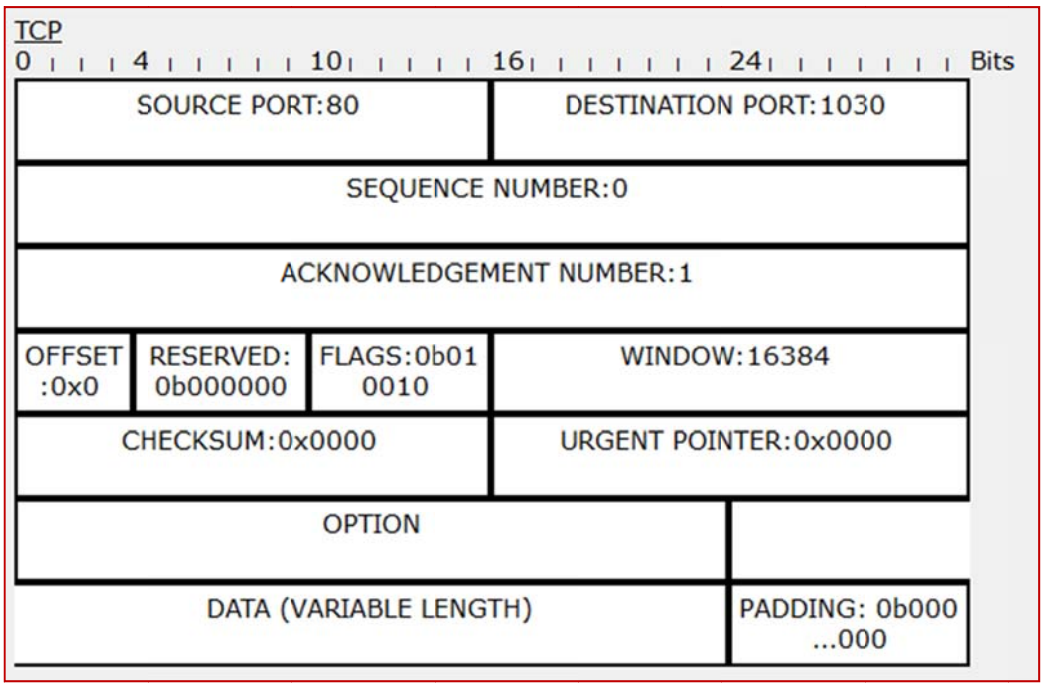


(2) 步驟 2：分析『客戶端建立連線』(Seq = 1)封包標頭，如下：



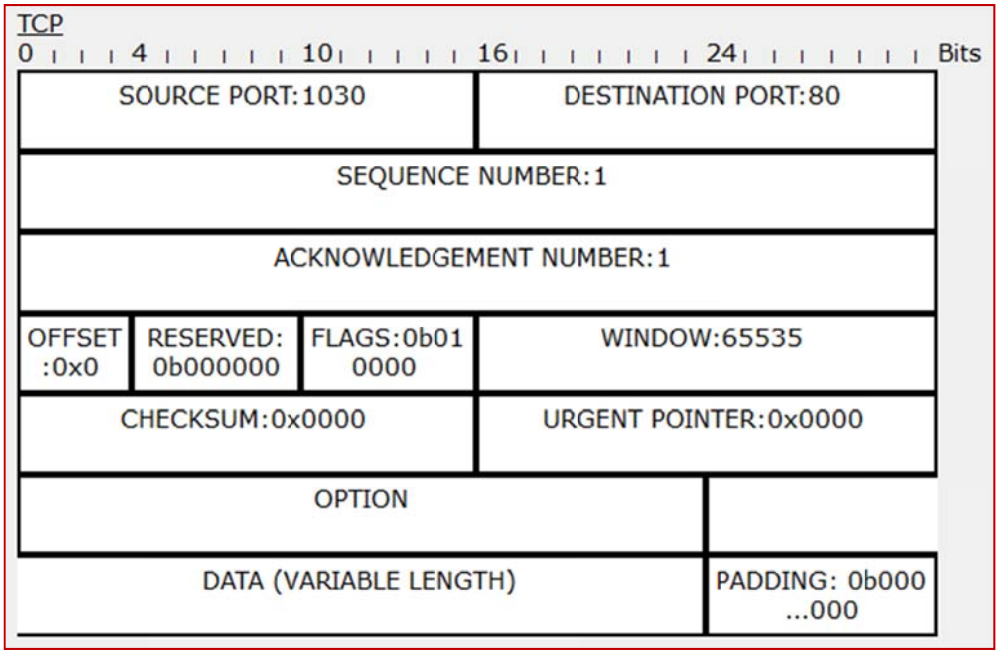
- Source Port = 1030、Destination Port = 80。
- Seq Num = 0、Ack Num = 0。
- Flags = 0b000010(0x02)(Syn = 1)。

(3) 步驟 3：分析『伺服端同意連線』(Seq = 1、Ack = 1)封包標頭，如下：



- Source Port = 80、Destination Port = 1030。
- Seq Num = 0、Ack Num = 1。
- Flags = 0b010010(0x12)(Ack = 1 & Syn = 1)。

(4) 步驟 4：分析**『客戶端確認連線』**(Ack = 1)封包標頭，如下：



- Source Port = 1030、Destination Port = 80。
- Seq Num = 1、Ack Num = 1。
- Flags = 0b010000(0x10)(Ack = 1)。

4-6 UDP 協定與分析

4-6-1 UDP 協定簡介

Internet 除了提供可靠性服務的 TCP 連接外，也提供非連接方式傳輸稱之為**『使用者電報傳輸協定』(User Datagram Protocol, UDP)**是**『非連接方式』(Connectionless)**。UDP 傳輸協定比 TCP 簡單，沒有連線要求、連線終止、以及流量控制的管理程序。它的優點是傳輸速率較快，主要應用於較少量、即時性傳輸，而對資料正確性的要求較不高 (如語音或視訊) 的環境下使用。而其缺點則是無法提供正確性較高的資料傳輸。採用 UDP 傳輸可能會有資料重覆、資料未依序到達、資料遺失等等問題，必須由使用者自行解決。但從一方面來思考，Internet 網路上有許多應用系統，它們之間的傳輸量很低，而且需要即時反映訊息，如果採用 TCP 連線反而會浪費許多連結時間，而影響傳輸效率，在這種情況之下使用 UDP 的效率相對應較高，譬如 DNS 伺服系統或 SNMP 協定。因此，可以做一個簡單的結論，再傳輸量比較少或需要及時反映的環境下，使用 UDP 協定傳輸會優於 TCP 協定。但在許多情況下，

使用者很難去決定到底應該使用何種協定來傳輸目前的資料，因此，在許多系統在同一傳輸埠口上，提供有 TCP 和 UDP 兩種協定讓使用使者連接，如果使用者的資料不需要分割，也就是說，一個 UDP 封包可以承載的話，那就使用 UDP 協定傳輸，如果需要多筆封包傳輸，則使用 TCP 協定傳輸。

UDP 封包與 IP 封包之包裝方式如圖 4-20 所示，圖 4-25 為 UDP 封包格式，因其為非連接方式，所以沒有順序號碼、確認號碼和其它控制欄位，而各欄位功能如下：

- **來源埠口（Source Port）：**發送端之傳輸埠口。
- **目的埠口（Destination Port）：**接收端之傳輸埠口。
- **長度（Length）：**該封包所承載資料（Data）的長度。
- **檢查集（Checksum）：**該封包之錯誤檢查的檢查集。

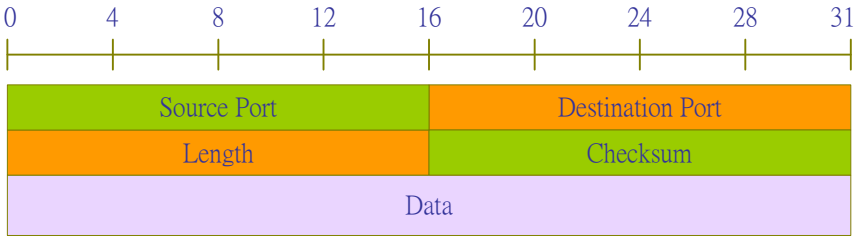


圖 4-25 UDP 之封包格式

至於『**檢查集**』欄位的產生就較為複雜，因此，有些應用環境為了提高效率，而將此欄位填入 0，而不使用錯誤檢查的功能。檢查集所檢查的範圍除了 UDP 標頭和所承載的資料外，還包含一些 IP 標頭的欄位，我們將所檢查的欄位組成一個稱之為『**虛擬標頭**』**(Pseudo Header)**，其內容如下：

- **IP Source Address：**(4 Bytes) IP 標頭之來源 IP 位址。
- **IP Destination Address：**(4 Bytes) IP 標頭之目的 IP 位址。
- **Protocol：**(1 Byte) IP 標頭之協定號碼欄位。
- **Length：**(2 Bytes) UDP 標頭之長度欄位。
- **Padding：**(1 Bytes) 補滿虛擬標頭成為偶數位元組長度，以方便計算 Checksum。

虛擬標頭的檢查方法是傳送端欲發送資料之前，首先建構虛擬標頭，再計算出檢查集的檢查碼，將其填入 UDP 的檢查集欄位，並捨棄虛擬標頭而不將其傳送過去。接收端收到 UDP 封包後，也再建立虛擬標頭來計算檢查碼，如果所計算出來的檢查碼和檢查集欄位的值相同，便判斷該 UDP 封包沒有發生錯誤。使用虛擬標頭檢查可視為 UDP 封包的雙重保全機制，如果封包在傳遞中發生錯誤，而下層通訊沒有檢查出來，虛擬標頭可以做第二道防線的檢查。

4-6-2 UDP 擷取與分析 - Wireshark

(A) 系統分析

採用 UDP 協定大多是訊息資料較短的應用，最常用的是 DNS 查詢訊息。當工作站欲連結某一個 URL(Uniform Resource Locator) 網址的主機時，它事先必須向 DNS Server 詢問該網址的 IP 位址，才可以利用該 IP 位址連結到該主機。詢問成功之後，工作站會將 URL 對應的 IP 位址儲存於 DNS cache 內，下次遇到同樣的 URL 名稱，就不需要再向 DNS Server 詢問。

因此，我欲利用 DNS 查詢擷取到 UDP 封包，必須先清除掉工作站內的 DNS cache (命令 ipconfig /flushdns)，再執行某一命令連結一個 URL 網址即可(執行 > ping www.tsnisn.idv.tw)。因 DNS cache 已被清除，工作站勢必發出 DNS 查詢訊息給 DNS Server。

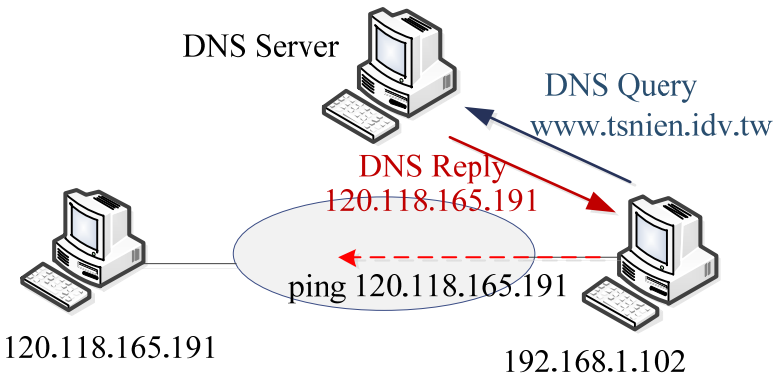


圖 4-26 UDP 封包擷取(ping www.tsnien.idv.tw)

(B) 擷取工具

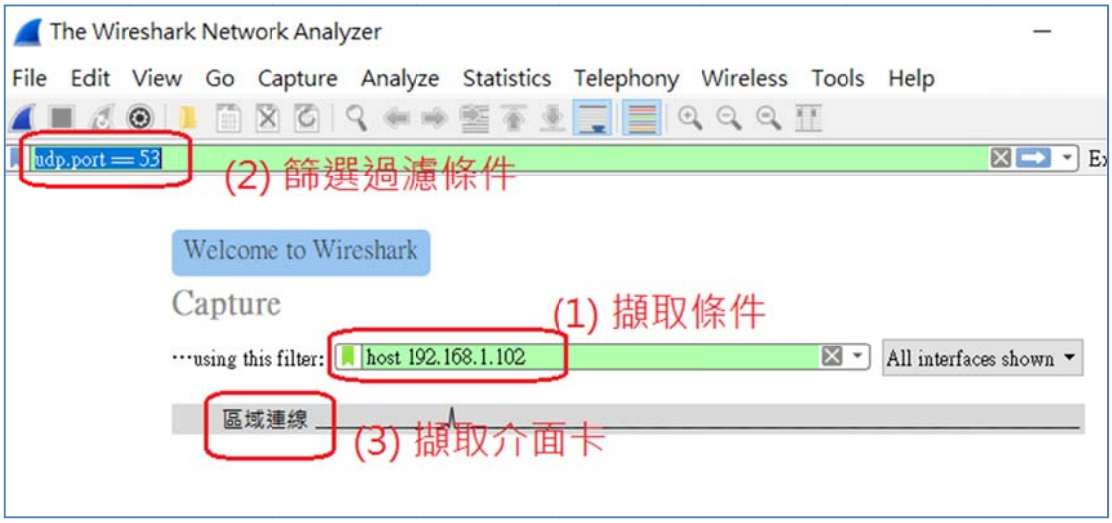
此實習題目，需要用到下列工具：

- Wireshark 網路封包分析器(安裝於 Windows 7)
- Windows 命令提示字元：
  - 命令 ipconfig /flushdns：清除 DNS 快取紀錄。
  - 命令 ipconfig /displaydns | more：顯示 DNS 快取紀錄內容。
  - 命令 ping www.tsnien.idv.tw：產生 DNS 查詢訊息，此為 UDP 協定封裝。

(C) 擷取封包步驟

(1) 開啟 Wireshark：

- 擷取條件：host 192.168.1.102 (windows IP)、
- 顯示篩選條件：udp.port==53、
- 再選擇介面卡，如下：



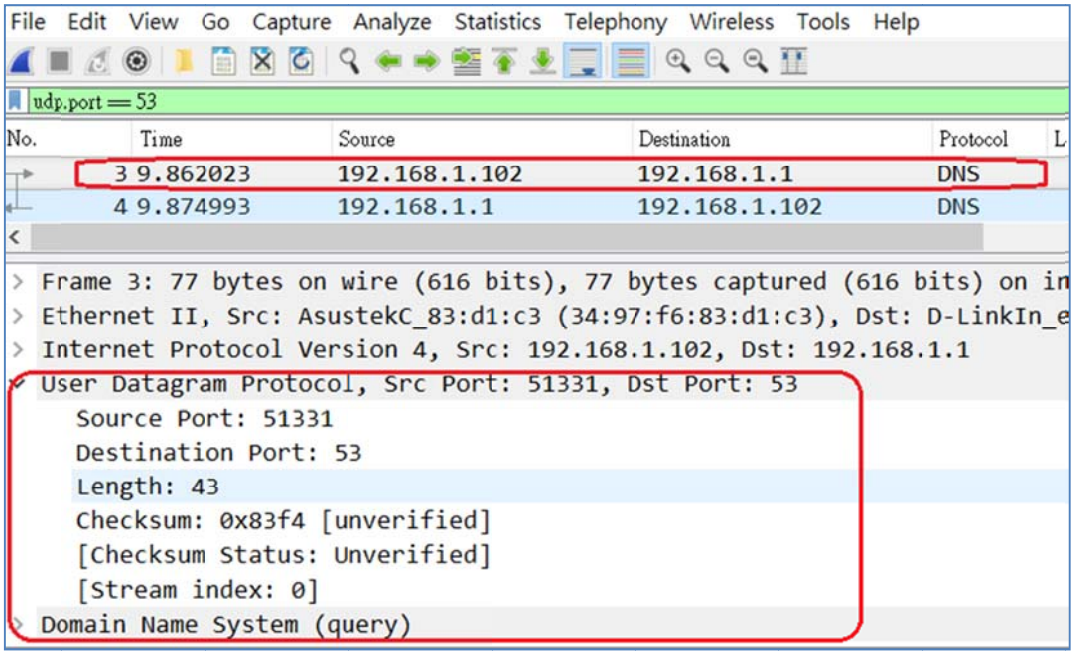
(2) 開啟 Windows 命令提示字元(**利用管理員身分開啟**)：

- 執行 > ipconfig /flushdns 命令、
- 執行 >ping www.tsnien.idv

(3) 在 Wireshark 視窗按暫停。

(D) UDP 協定分析

圖中第 3 封包是主機(192.168.1.102) 發出的第一個 DNS 查詢訊息，該網路的 Default Gateway 是 192.168.1.1，因此，需由這裏出去。其 UDP 封包標頭的各欄位分析如下：



- Source Port：51331
- Destination Port：53 (DNS 服務埠口)
- Length：43
- Checksum：0x83f4
- Data：Domain Name System(query)

4-6-3 UDP 擷取與分析 – Packet Tracer

(A) 系統分析

採用 UDP 協定大多是訊息資料較短的應用，最常用的是 DNS 查詢訊息。當工作站欲連結某一個 URL 網址的主機時，它事先必須向 DNS Server 詢問該網址的 IP 位址，才可以利用該 IP 位址連結到該主機。詢問成功之後，工作站會將 URL 對應的 IP 位址儲存於 DNS cache 內，下次遇到同樣的 URL 名稱，就不需要再向 DNS Server 詢問。

因此，我欲利用 DNS 查詢擷取到 UDP 封包，必須先清除掉工作站內的 DNS cache (命令 ipconfig /flushdns)，再執行某一命令連結一個 URL 網址即可(執行 > ping PC1..tsnisn.idv.tw)。因 DNS cache 已被清除，工作站勢必發出 DNS 查詢訊息給 DNS Server。

(B) 網路規劃

吾人利用 Packet Tracer 設計一個簡單網路，包含有三個 PC 電腦，期望網路環境如下：

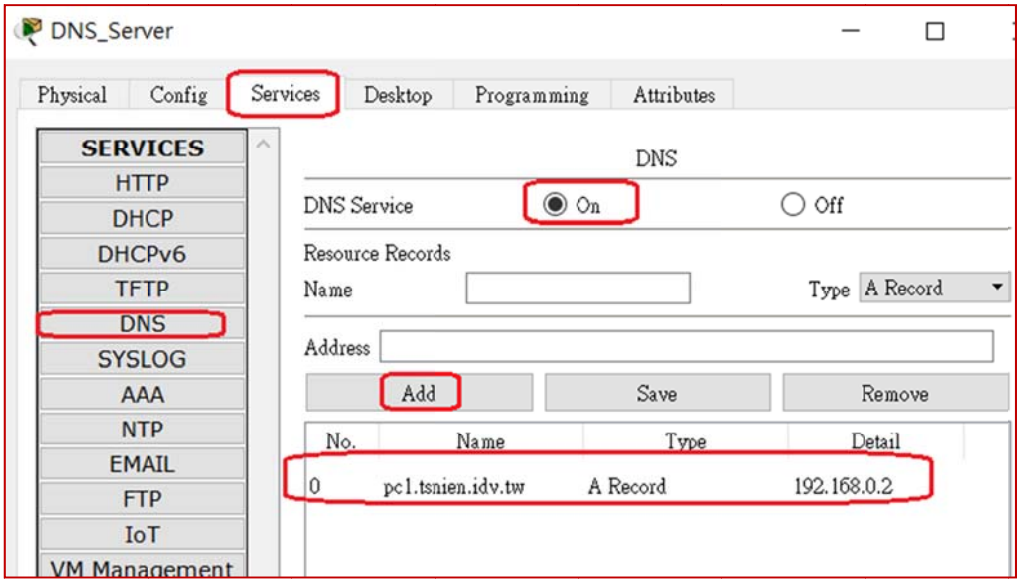
網路區段	Gateway/DNS	名稱	IP 位址	連接埠口
192.168.0.0/ 255.255.255.0	192.168.0.254/ **192.168.0.250**	PC0	192.168.0.1	HUB(Fa0)
		PC1(pc1.tsnien.idv.tw)	192.168.0.2	HUB(Fa1)
		DNS_Server	192.168.0.250	HUB(Fa5)

因此，我們需要在 Packet Tracer 上選擇下列裝置：

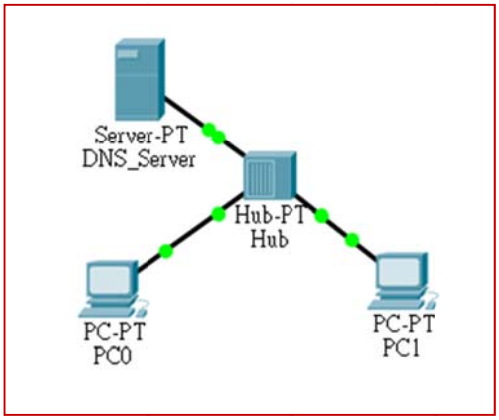
(1) Hub-PT：模擬集線器 (Hub) 一只。提供 PC 電腦之間連線。

(2) PC-PT：模擬 PC 主機二只。PC0 與 PC1 主機使用。

(3) Server-PT：模擬伺服器主機一只。開啟 DNS Service，並增加一筆位址資源紀錄 (pc1.tsnien.idv.tw = 192.168.0.2)， 如下：



(4) 規劃網路如下：**(請下載 UDP 封包擷取.pkt)**



(C) 網路設定

- 集線器 Hub 不需任何設定。
- PC0 與 PC2 須設定相關網路參數，如下(如 PC0)：Gateway = 192.168.0.254、DBS Server = 192.168.0.250、IP Address = 192.168.0.1、Subnet Mask = 255.255.255.0。
- DNS_Service：Gateway = 192.168.0.254、DBS Server = 192.168.0.250、IP Address = 192.168.0.250、Subnet Mask = 255.255.255.0。

(D) 擷取封包步驟

(1) 步驟 1：Packet Tracer 採用 Simulation 模式，編輯 Edit Filters ，點選 UDP，表示只擷取 UDP 封包。

(2) 步驟 2：先在 PC0 上清除 DNS Cache，再 ping www.pc1.tsnien.idv.tw，如下：

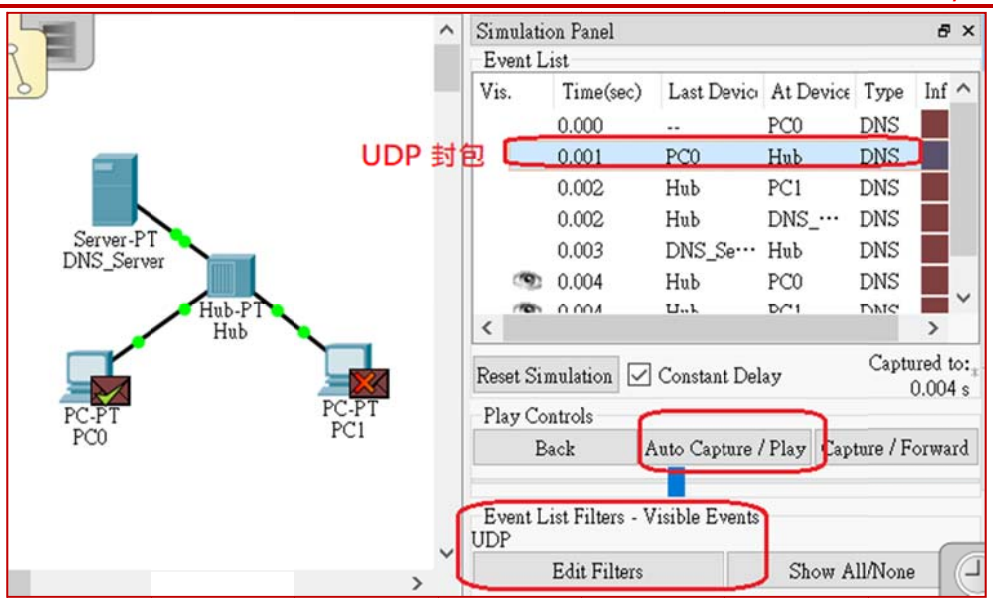
```
C:\>ping pc1.tsnien.idv.tw

Pinging 192.168.0.2 with 32 bytes of data:
```

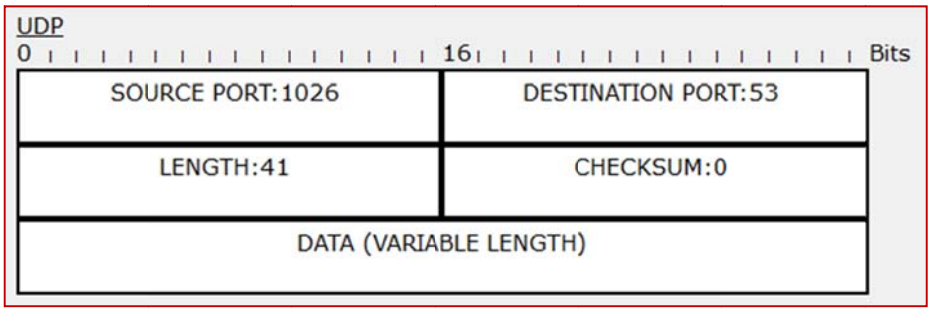
(3) 步驟 3：在 packet Tracer 上按『Auto Capture/Play』暫停。

(E) UDP 協定分析

(1) 步驟 1：在 Packet Tracer 按 『Auto Capture/Play』，則可觀察到擷取到 UDP (DNS 封包) 的封包。



(2) 步驟 2：分析 UDP 封包標頭，如下：



- Source Port = 1026、Destination Port = 53。
- Length = 41、Checksum =0。