修平技術學院

資訊網路技術系

IEEE 802.11 無線區域網路
通訊協定與 802.11 封包解析

指導老師:**張永昌** 老師

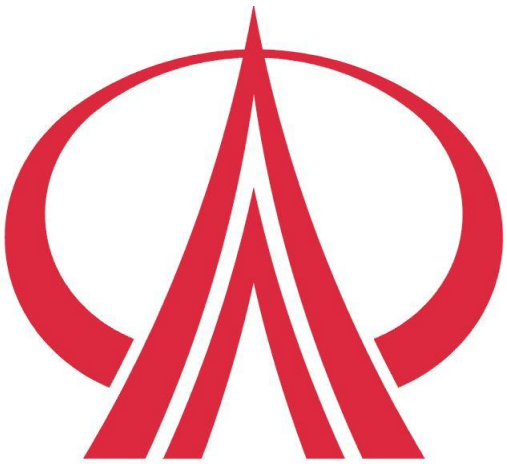
學生:劉鎧境 BN94009
學生:張家賓 BN94010
學生:陳毅福 BN94063

中 華 民 國　　九十八　年　一　月

資訊網路技術系 專題報告

IEEE 802.11 無線區域網路

通訊協定與 802.11 封包解析



指導老師:_____**張永昌**_____

評審老師:_____張永昌_____
_____陳振庸_____
_____麥毅廷_____

目 錄

圖目錄

表目錄

第一章 摘要與前言

摘 要

近年來隨著資訊科技的發展,無線網路的盛行使人們上網不需受網路線所限制,國內許多公共場所也已經開始在進行無線網路(Wireless Network)的建置,包括許多學校也都開始投入校園無線網路的建置實驗,因此IEEE 802.11 就這樣開始興起,搶攻了國內大部份的市場,免佈線的便利性與高移動性,使得人們願意將公司或家裡的網路升級成無線網路,走到哪裡都可以四處上網。

然而建置無線網路進行上網時,難免都會遇到錯誤的情形,因此本專題是透過 WireShark 軟體來進行無線網路封包的解析,來排除掉網路連線的故障問題,首先一開始要先進行無線網路的對等式(Ad Hoc)與主從式(Infrasturcture)架構的建置實驗,這樣才可利用 WireShark 軟體所擷取下來的封包進行分析,進而避免掉網路連線的故障問題。

前 言

1.動機與目的

由於現在的無線網路,是任何使用者只要帶著 Notebook 筆記型電腦在無線網路的服務環境，就能享用所有的網路服務，所以只要有 Notebook 筆記型電腦和一片 IEEE 802.11 的無線網卡(例如~實驗中所用的 AirPcap)，搭配著桌上型電腦的有線網路，就能使用到無線網路的服務。

隨著資訊科技的進步，無線網路的技術已經漸漸成熟與相關產品的推出，使得有越來越多的使用者希望使用無線網路來上網,而不再受到網路線的限制，然而無線網路所建置的模式，也能由基本的對等式(Ad Hoc)與主從式(Infrasturcture)衍生出多組不同的架構,因此本專題的目的是在於能夠掌握區域無線網路不同架構的建置，並能透過無線網路封包解析軟體 WireShark 來進行網路問題的判斷和故障的排除。

第二章 背景知識介紹

2.1 網路封包擷取軟體

網路封包的分析是經常用來解決設備不足的最佳方案。分析網路封包，除了能看出網路流量和找出異常之外，也能用來學習不同通訊協定。目前常見的網路封包分析工具有Tcpdump、Sniffer、NetXRay、WireShark(Ethereal)‧‧‧‧等。

其中WireShark的前身就是Ethereal，它是一個開放原始碼的封包分析軟體，能夠快速的更新，且WireShark能解析七百種以上的通訊協定，幾乎所有的協定都能夠解碼，就算將來有新的通訊協定推出，也會因為開放原始碼的授權方式，而能夠迅速地發展出新通訊協定所需的程式。

WireShark具備優異的底層協議分析能力，特別是封包過濾器的功能靈活強大，使用者可以針對特定的封包目標作分析，有助於通訊協定異常行為的偵測與分析。圖形化的介面能顯示出每一層封包的詳細訊息，能讓使用者相當容易上手，並可以輕鬆的瀏覽封包內容，支援UNIX/Linux 和 Windows等多項平台，可以搭配AirPcap無線網卡一起使用。

如下圖所示，WireShark提供圖形化的操作介面和功能完整強大的過濾器，能讓使用者快速地找到想要分析的封包訊息。其內建的通訊協定解析功能，也可以讓使用者掌握每一個網路封包的詳細資訊。使用者能經由過濾器(Filter)輸入關鍵字或條件，協助鎖定接下來要分析的目標。在Filter的條件欄位內，若底色呈現綠色，就表示輸入的語法正確；反之則會呈現紅色的底色。

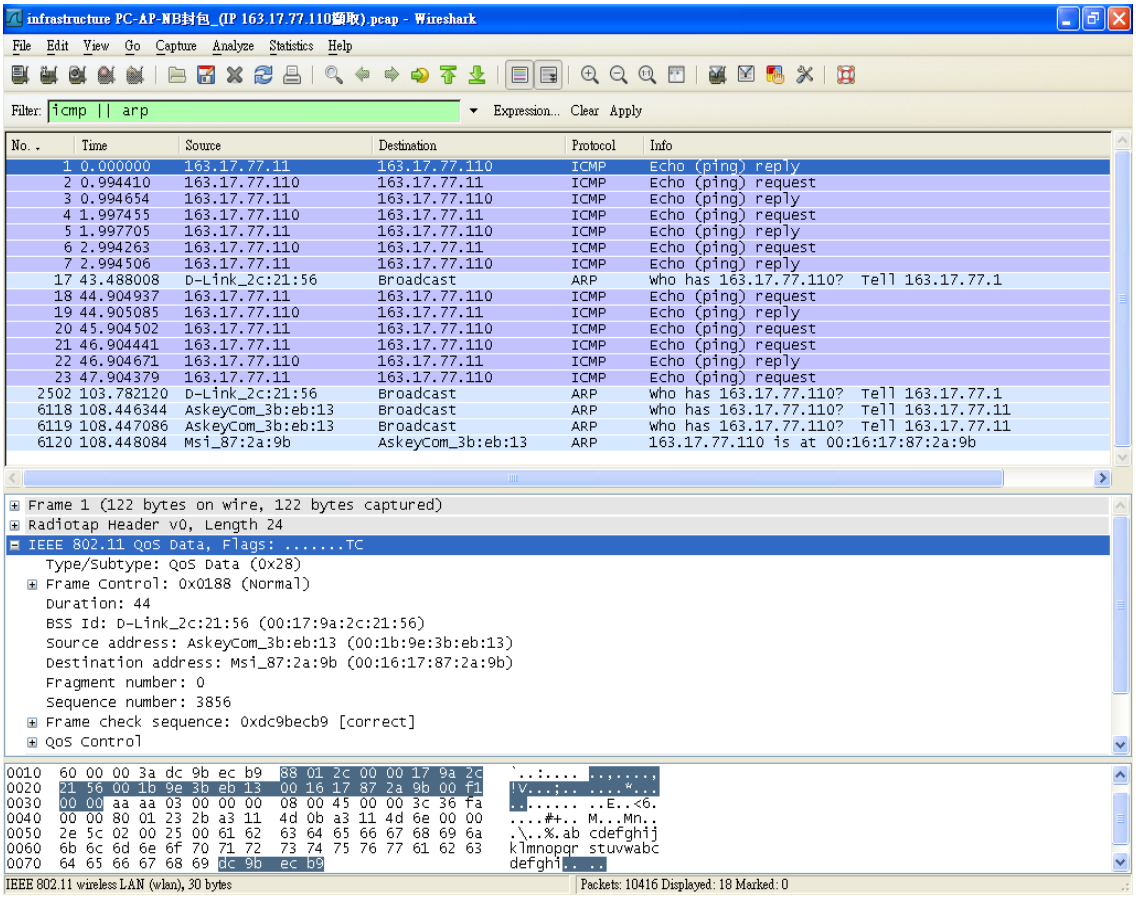


圖2.1.1 WireShark圖形化操作介面

2.2 IEEE 802.11架構與簡介

依據 IEEE802.11b 標準協定，無線網路共定義為下列二種模式

- Ad Hoc
- Infrastructure

Ad Hoc 無線網路模式下使用無線網路卡的電腦BSS(Basic Service Set)，可透過無線網路卡與其他的電腦互相溝通形成網路，但此一模式則無法連接Internet

圖2.2.1 Ad Hoc 無線網路模式

Infrastructure 無線網路模式下使用無線網路卡的電腦必需透過AP (Access Point)做為與其他的電腦互相溝通形成網路並與乙太網路(有線網路)電腦連接，即可連接Internet

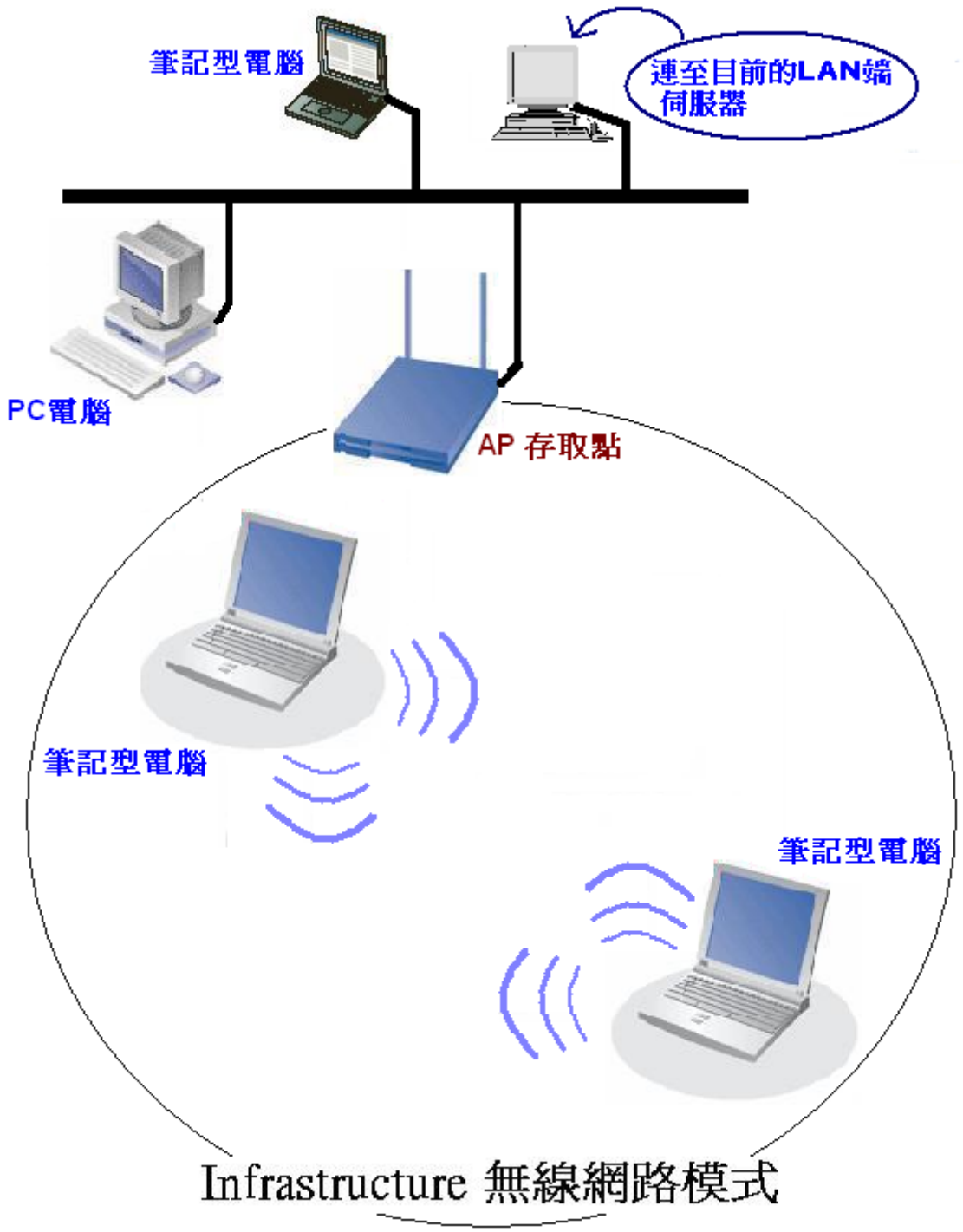


圖 2.2.2 Infrastructure 無線網路模式

2.3 無線網路之名詞介紹

Access Point

就是無線存取橋接器(簡稱AP)，是傳統的有線區域網路與無線區域網路或無線區域網路與無線區域網路之間的橋樑，且用來"接收和傳送"資料；任何一台裝有無線網路卡的PC電腦均可通過AP來分享有線區域網路甚至廣域網路的資源。AP本身又可對裝有無線網路卡的PC作必要的控制和管理。

Internet Protocol Address

如同網路上的地址一般，簡稱為IP位址，在網際網路TCP/IP架構中，每台電腦主機都必須有"獨一無二的IP(Internet Protocol)位址"，定義著網路上的每一節點，以識別不同的電腦主機身分，如此才能在網路上依照IP位址，正確的傳遞及接收資料。

SSID

SSID全名為Service Set Identifier(服務設置識別碼)，是指你的AP在網路上的名稱，用來識別無線區域網路的身份認證機制。為一群無線區域網路裝置所共用的網域名稱，只有使用相同SSID的裝置才能建立連線。

命令提示字元指令

ipconfig

可顯示目前所有網路卡TCP/IP的網路設定值，並重新整理動態主機設定通訊協定(DHCP)及網域名稱系統(DNS)設定。

ping

藉由傳送網際網路控制訊息通訊協定(ICMP)的回應要求訊息，驗證到其他 TCP/IP 電腦的 IP 和連線，用來偵測網路上的遠端主機是否存在，並判斷網路是否正常的偵測工具。

第三章 實作方法與步驟

3.1 Ad Hoc 架構模擬與設定

Ad Hoc 對等式無線網路架構

1.進入無線網路連線的內容，點右鍵開啟「TCP/IP 內容」，設定兩台 Notebook（NB 筆記型電腦）相同網段的 IP 位址，如下

NB 筆記型電腦 a → IP 位址設定成：192.168.0.11

子網路遮罩設：255.255.255.0

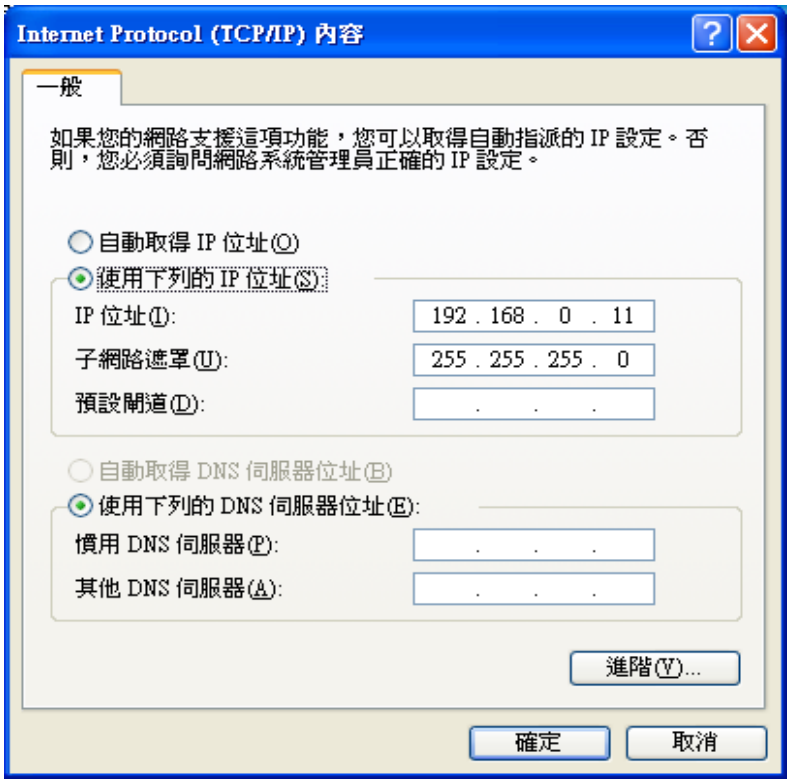


圖 3.1.1 Ad Hoc 架構 IP 位址- NB 筆記型電腦 a

NB 筆記型電腦 b → IP 位址設定成：192.168.0.22

子網路遮罩設：255.255.255.0

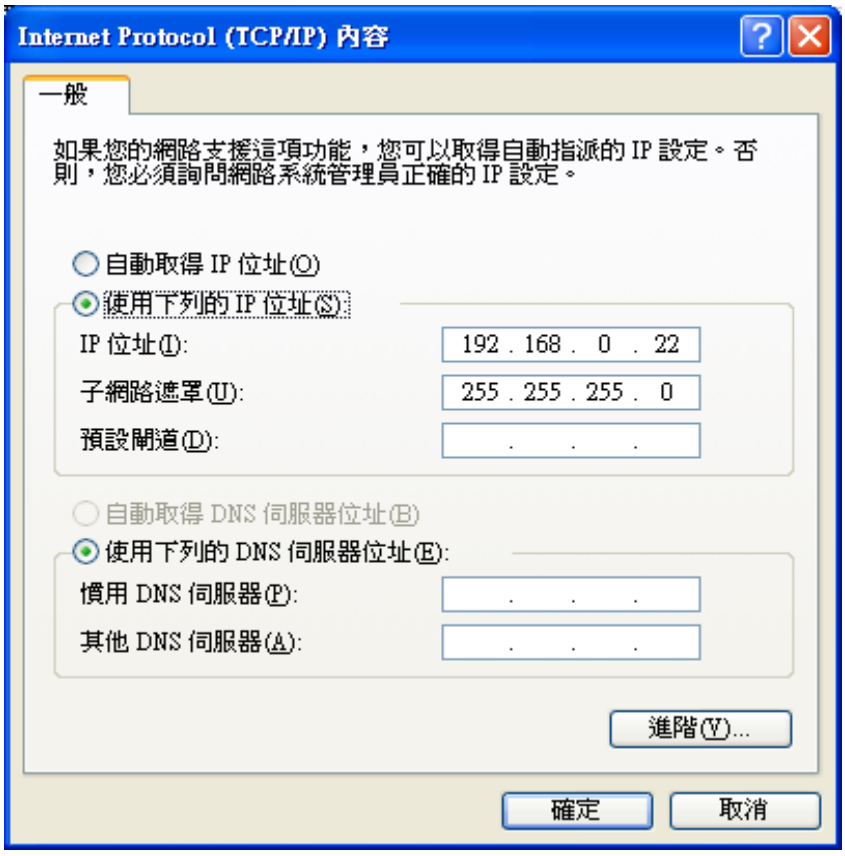


圖 3.1.2 Ad Hoc 架構 IP 位址- NB 筆記型電腦 b

2.在視窗中點選上方的無線網路標籤，按「進階」鈕將網路設定成 ad hoc 模式

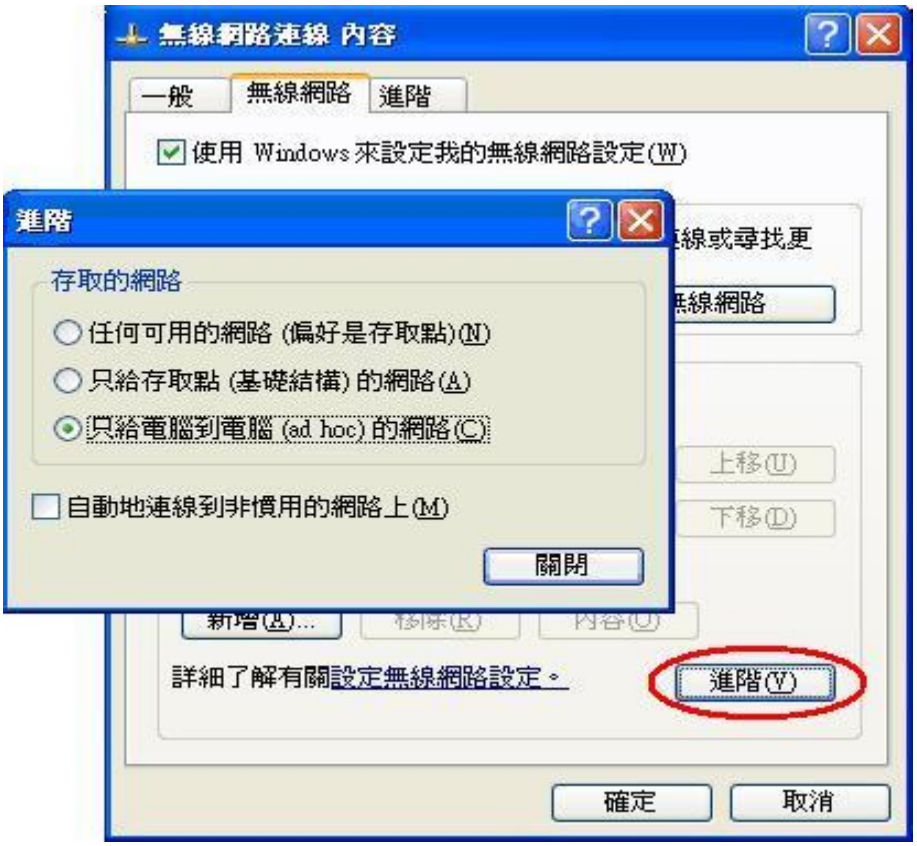


圖 3.1.3 存取的網路架構 Ad Hoc

3.在視窗中點選內容，設定網路名稱(SSID)和資料加密，如下

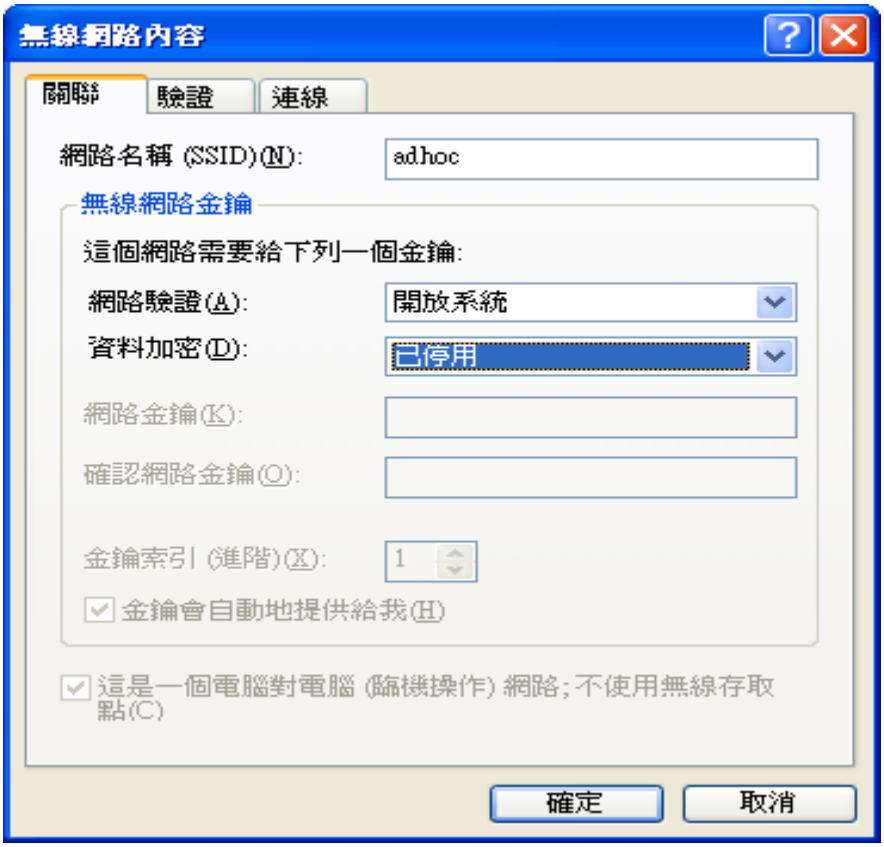


圖 3.1.4 Ad Hoc 網路名稱(SSID)設定

4.SSID 建立完畢，按下確定後會顯示“ad hoc (自動)”的圖示，代表成功建立且會自動連結

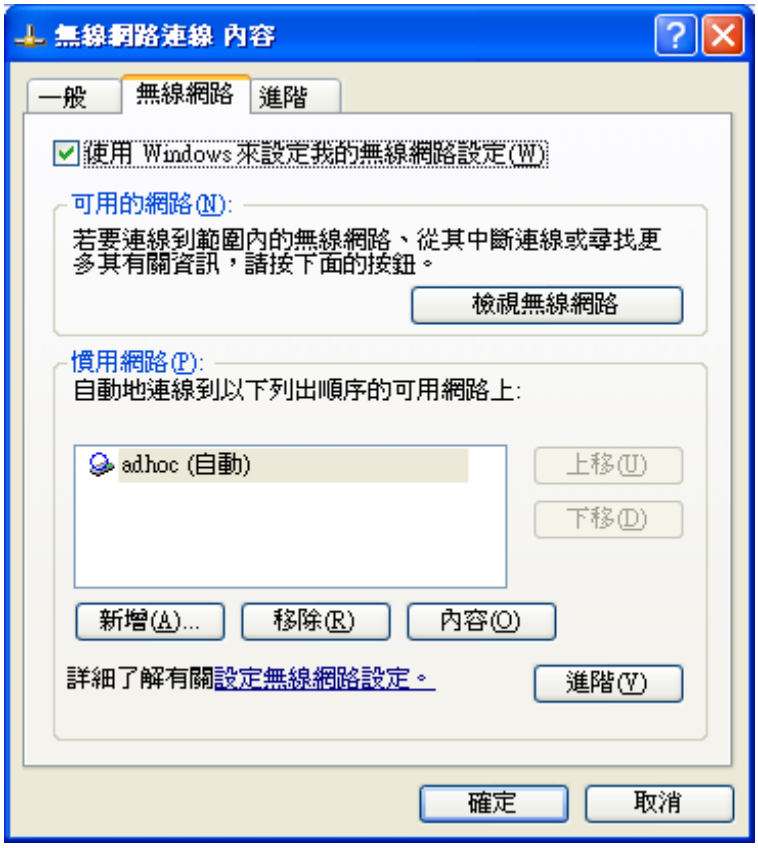


圖 3.1.5 已設定的 SSID 名稱

5.進入網路連線的視窗，在無線網路連線的圖示上按右鍵點選「檢視無線網路」開啟視窗畫面，如下圖。 在視窗左方點選重新整理網路清單，等待先前設定的 SSID 名稱（ad hoc）出現在清單後，點選 ad hoc 進行連線。

圖 3.1.6 Ad Hoc 架構 「無線網路連線」視窗

6.進入執行的視窗，輸入 cmd 指令開啟命令提示的畫面，使用關鍵字 ping 的指令檢查是否與另一台 Notebook 電腦接通了，如下

NB 筆記型電腦 a → 指令：ping 192.168.0.22 →(另一台筆記型電腦的 IP 位址)

由執行的輸出結果可看出 NB 筆記型電腦 a 順利的與另一台電腦接通了！

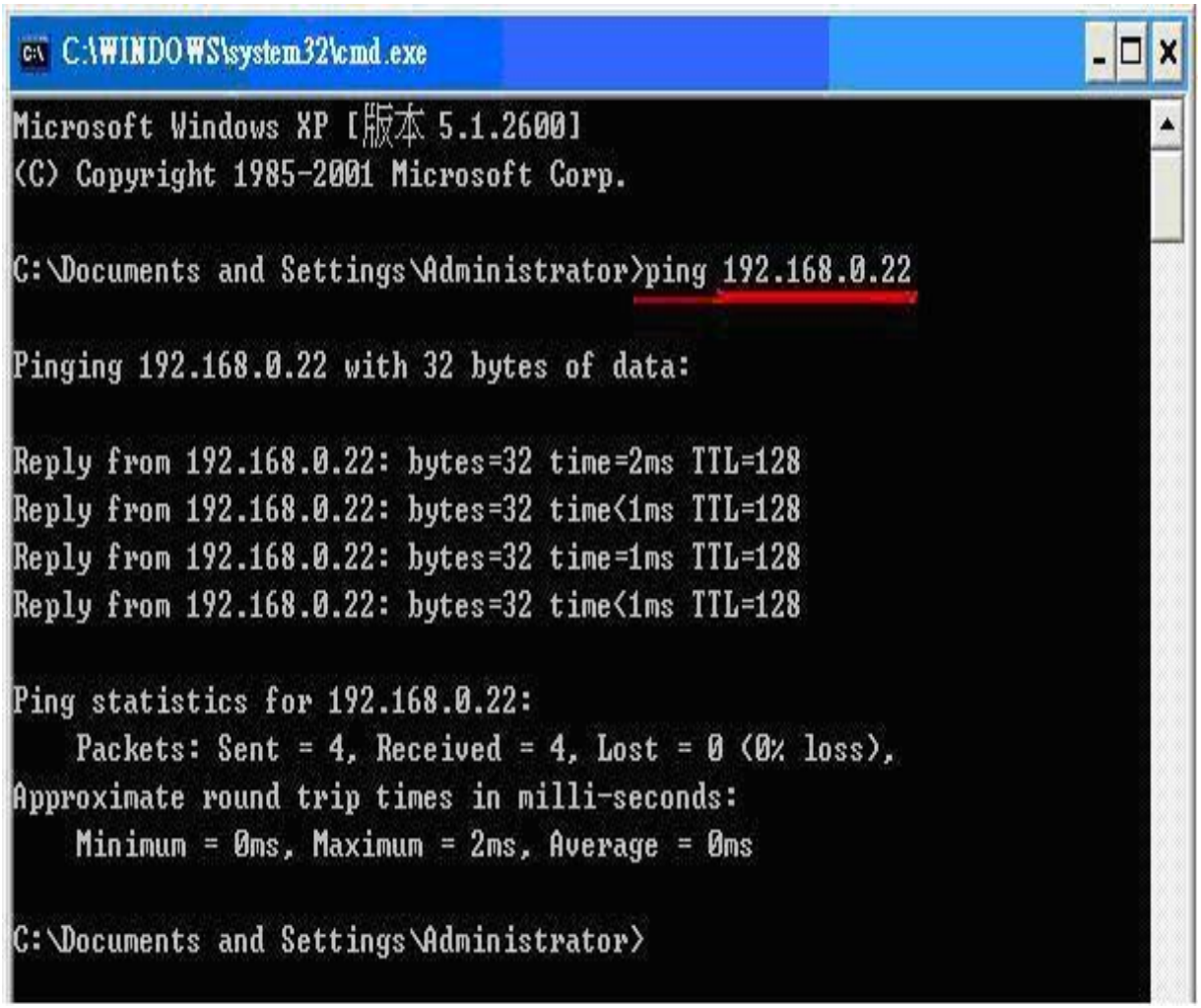


圖 3.1.7 Ad Hoc 架構 命令提示視窗-NB 筆記型電腦 a

NB 筆記型電腦 b → 指令：ping 192.168.0.11 →(另一台筆記型電腦的 IP 位址)

由執行的輸出結果可看出 NB 筆記型電腦 b 順利的與另一台電腦接通了！

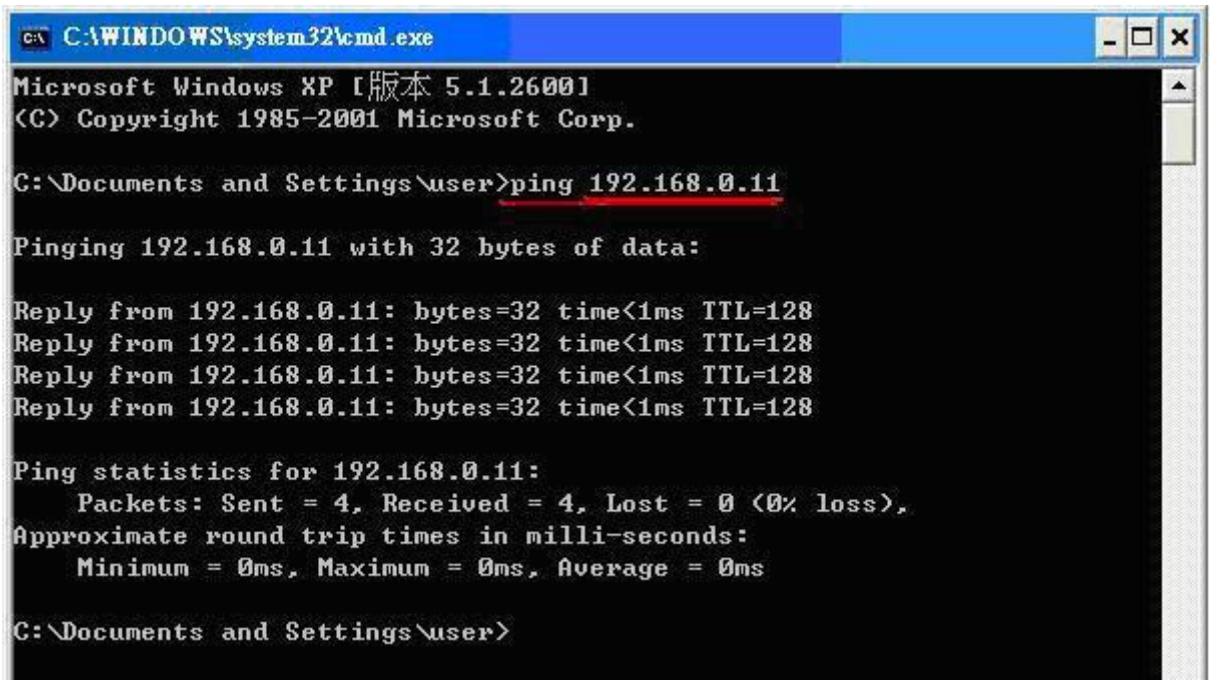


圖 3.1.8 Ad Hoc 架構 命令提示視窗-NB 筆記型電腦 b

7.在兩台 NB 筆記型電腦中點選資料夾，設定成共用模式，將檔案資料提供給另一台電腦存取使用，如下

8.進入網路上的芳鄰在左方電腦名稱，輸入另一台 Notebook 電腦的 IP 位址，進行搜尋存取檔案資料，如下：

NB 筆記型電腦 a → 搜尋：192.168.0.22　→(另一台筆記型電腦的 IP 位址)

(a) 搜尋結果的輸出畫面

圖 3.1.9 Ad Hoc 架構 搜尋結果-NB 筆記型電腦 a

NB 筆記型電腦 b →搜尋： 192.168.0.11 →(另一台筆記型電腦的 IP 位址)

(a)搜尋結果的輸出畫面

圖 3.1.10 Ad Hoc 架構 搜尋結果-NB 筆記型電腦 b

(b)NB 筆記型電腦 b 進入 IP 位址 192.168.0.11 進行檔案資料存取

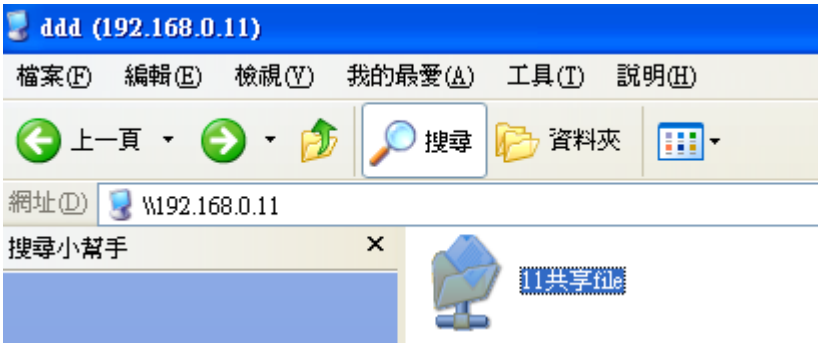


圖 3.1.11 Ad Hoc 架構 檔案資料存取

8.一開始先在 NB 筆記型電腦安裝 Air Pcap 的驅動程式還有 WireShark 軟體，安裝完成之後，在 NB 筆記型電腦 a 插入 Air Pcap 無線網卡後，再開啟的 WireShark 封包擷取軟體，點選上方 Capture→ 開啟 Interfaces 視窗畫面，選擇 AirPcap 的網卡介面，按下 Start 按鈕開始擷取封包，如下圖

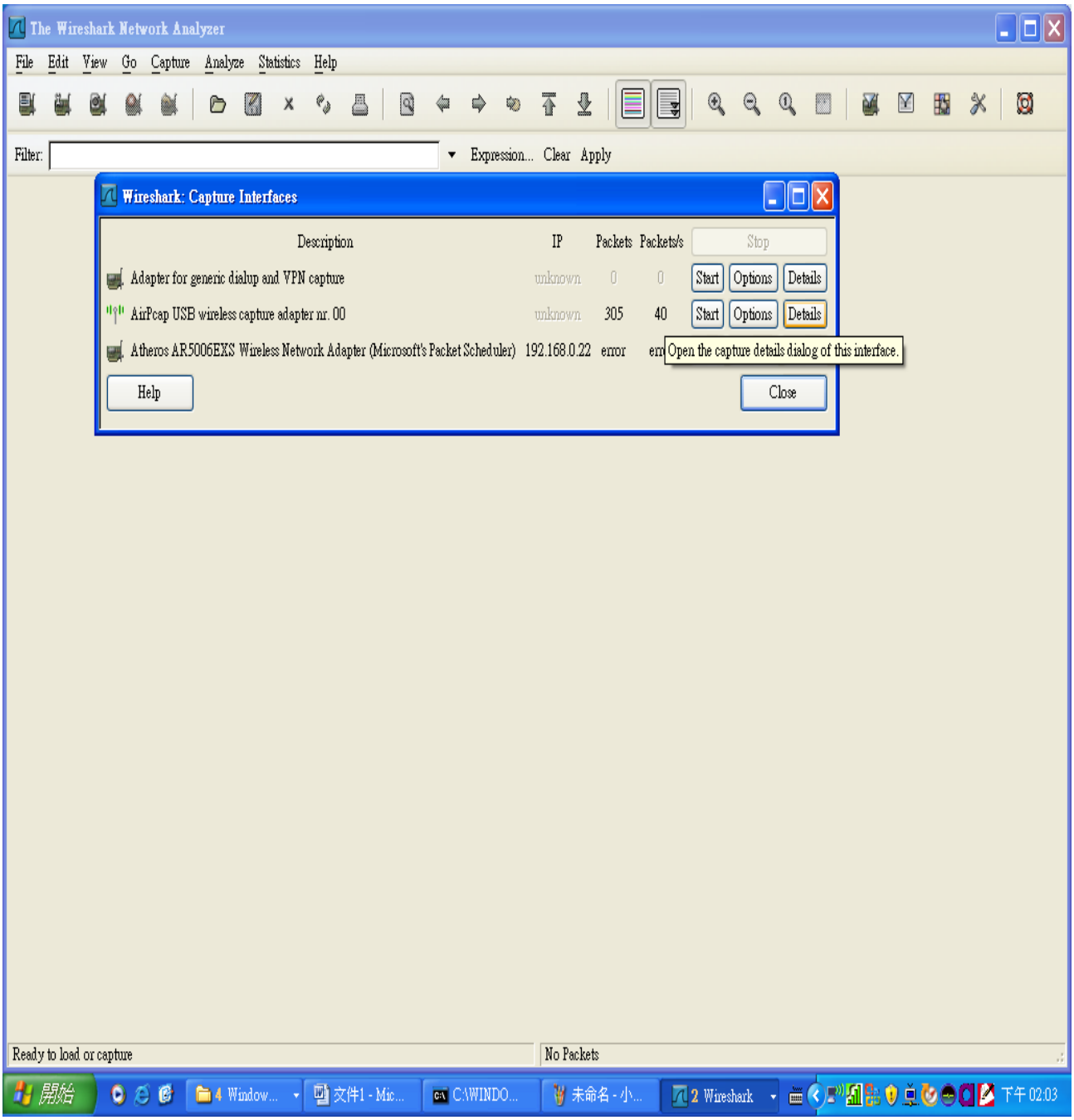


圖 3.1.12 Ad Hoc 架構 封包擷取前的設定-NB 筆記型電腦 a

9.在上半段的封包擷取畫面中，將會看見許多包含有自己的和外界的封包，而從右方 Info 欄位訊息的 SSID 名稱當中，即可判斷出來。 在下半段的封包資訊當中，將可在 IEEE 802.11 的展開畫面當中，看見 NB 筆記型電腦 a 與另一台筆記型電腦互傳檔案時的 16 進位封包資料。

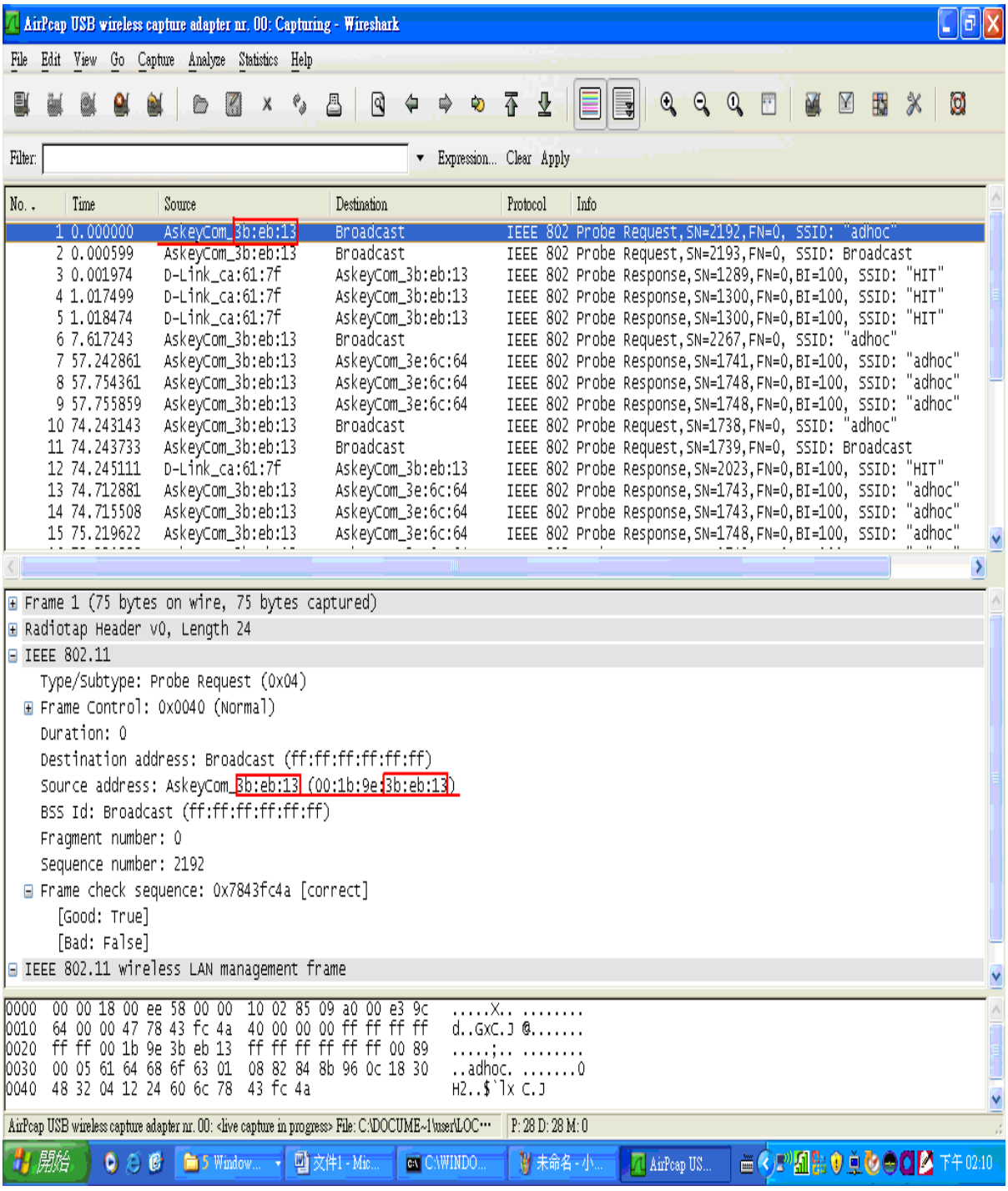


圖 3.1.13 Ad Hoc 架構 封包擷取結果-NB 筆記型電腦 a

10.進入 NB 筆記型電腦 b 的 WireShark 封包擷取軟體，點選上方 Capture→ 開啟 Interfaces 視窗畫面，按下選定的 AirPcap 網卡介面的 Options 按鈕開始作封包過濾設定。

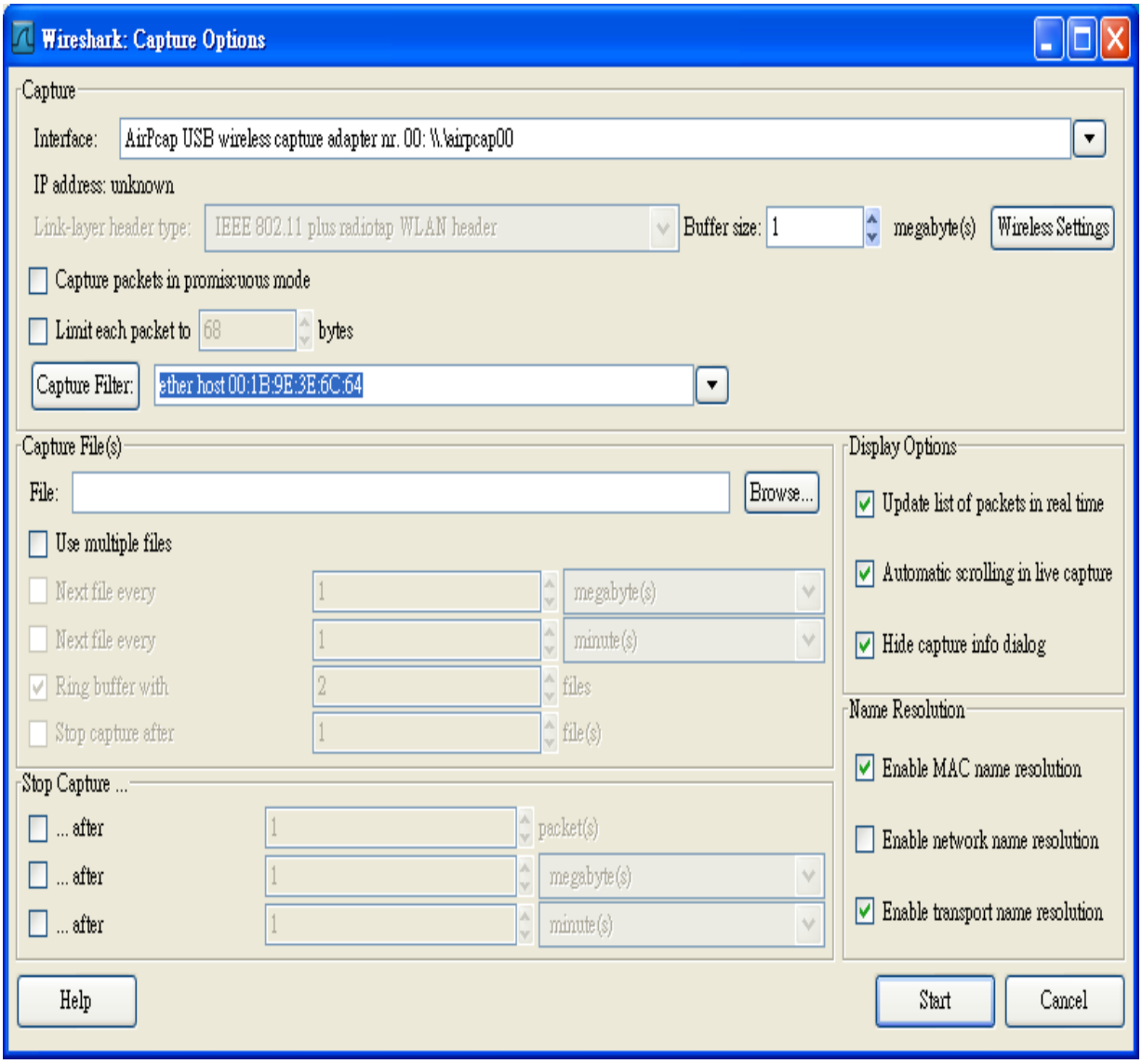


圖 3.1.14 Ad Hoc 架構 封包擷取前的設定-NB 筆記型電腦 b

11.在這上半段的封包擷取畫面中，同樣看見許多包含有自己的和外界的封包。 在下半段的封包資訊當中，同樣在 IEEE 802.11 的展開當中，看到 NB 筆記型電腦 b 與另一台筆記型電腦互傳檔案時的 16 進位封包資料。

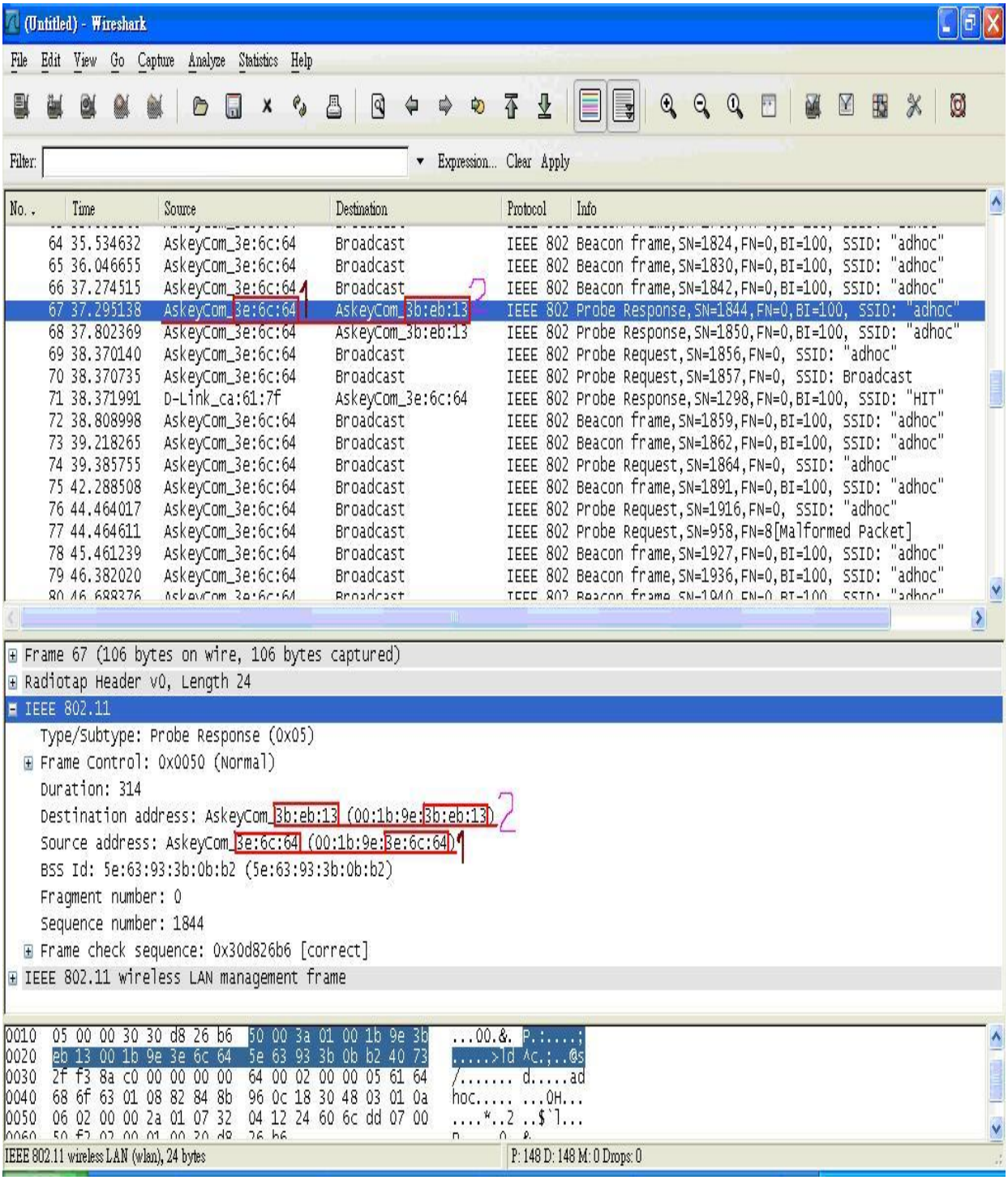
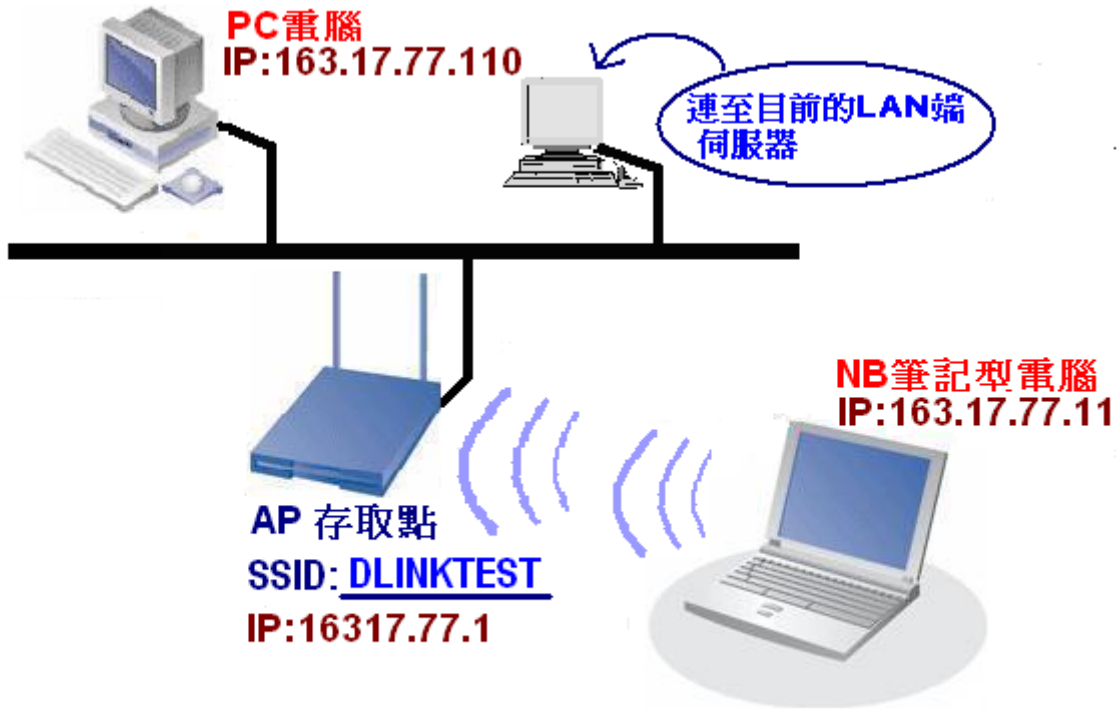


圖 3.1.15 Ad Hoc 架構 封包擷取結果-NB 筆記型電腦 b

3.2 Infrastructure 模式-透過「1 台」AP 互連



Infrastructure 無線網路模式(AP*1台)

3.2.1 PC 設定模式

1.先開啟網路上的芳鄰，再點選資料夾左邊的檢視網路連線點進去(或是在網路上的芳鄰點選右鍵按內容就能看見網路連線視窗了)，然而開啟區域連線設定(如~畫面中數字標示 1)，就會跑出個區域連線狀態視窗，再點選下面的內容按鈕，會跑出個區域連線內容視窗，在連線使用項目那裡拉到最下面點選 Internet Protocol(TCP/IP) 打開(如~畫面中數字標示 2)，輸入適合您電腦的 IP 位址，如下

PC 電腦 →IP 位址設定成：163.17.77.110

子網路遮罩設：255.255.255.0

預設閘道設：163.17.77.254

慣用 DNS 伺服器：163.17.64.30─→(如~畫面中數字標示 3)

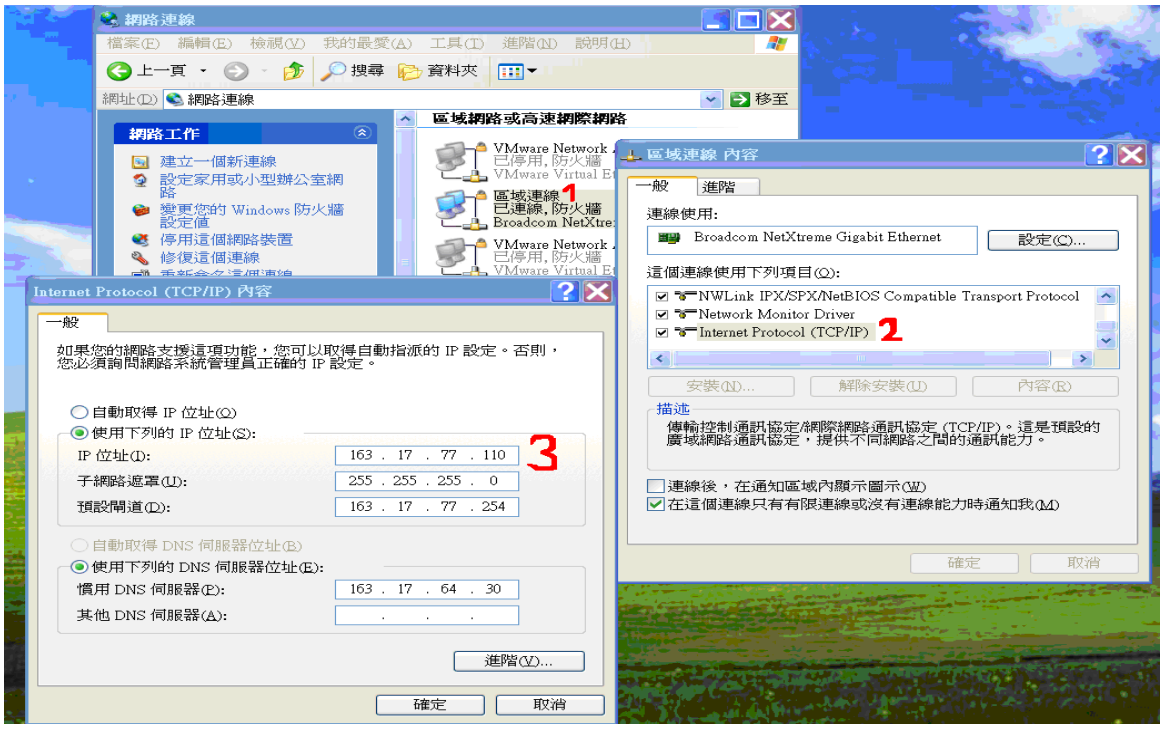


圖 3.2.1 Infrastructure 模式 IP 位址設定-PC 電腦

2.首先先開網頁，然後進到 AP 的設定畫面，預設通常是 192.168.0.1，在網址欄那裏輸入即可進入。(但此預設 IP:192.168.0.1 是可以進去 AP 設定頁面更改，如下圖中所輸入的 IP 就不是以 192.168.0.1 進去 AP 設定頁面)。

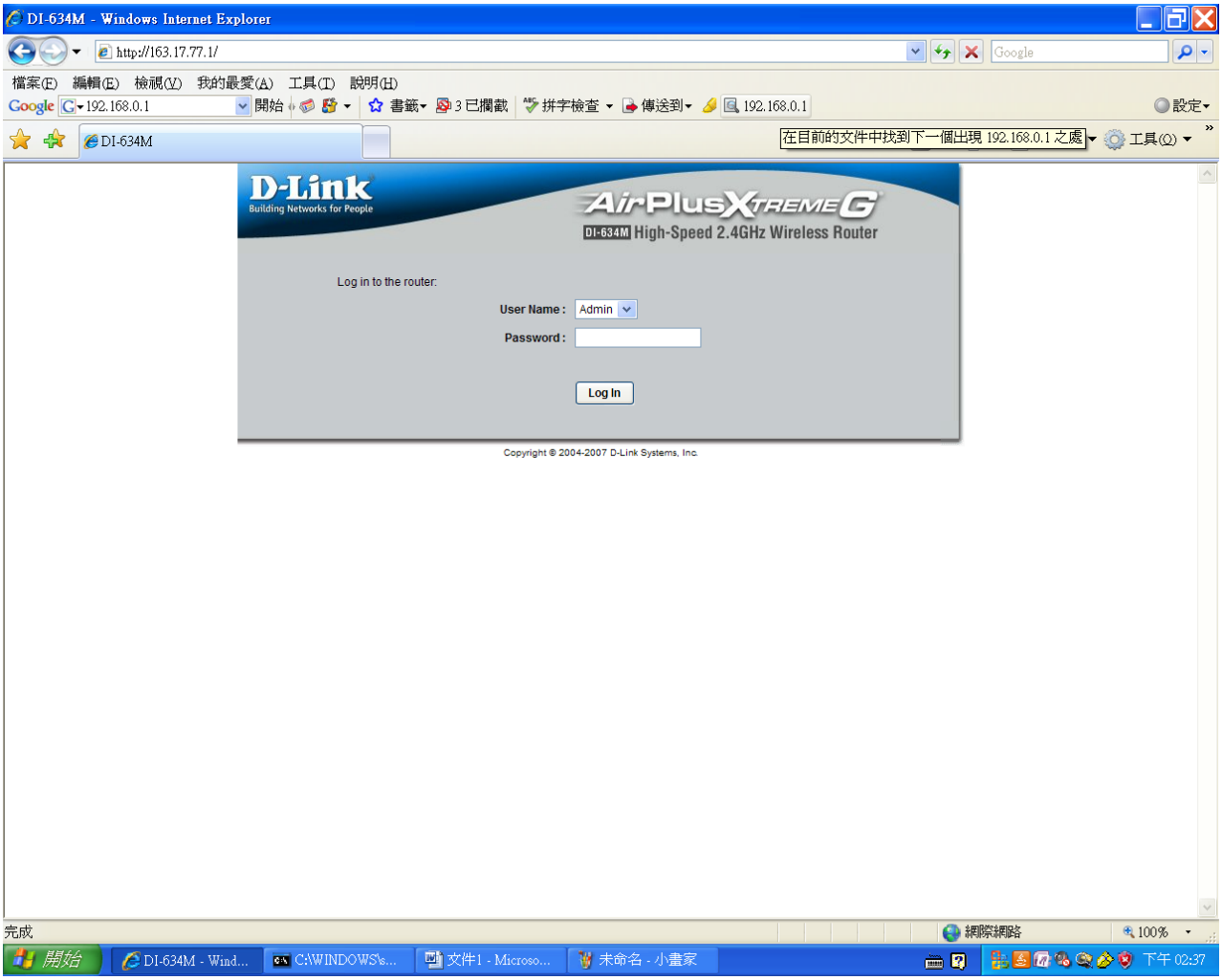


圖 3.2.2 Infrastructure 模式 AP 設定視窗

3.進入 AP 設定頁面後，點選上面一排中的Home 選項，在選取左邊欄位選項中的 Wireless 便可以來到設定 SSID 的畫面，在 SSID 欄位輸入您想設定的名稱即可，然後在點擊下面的 Apply 按鈕。

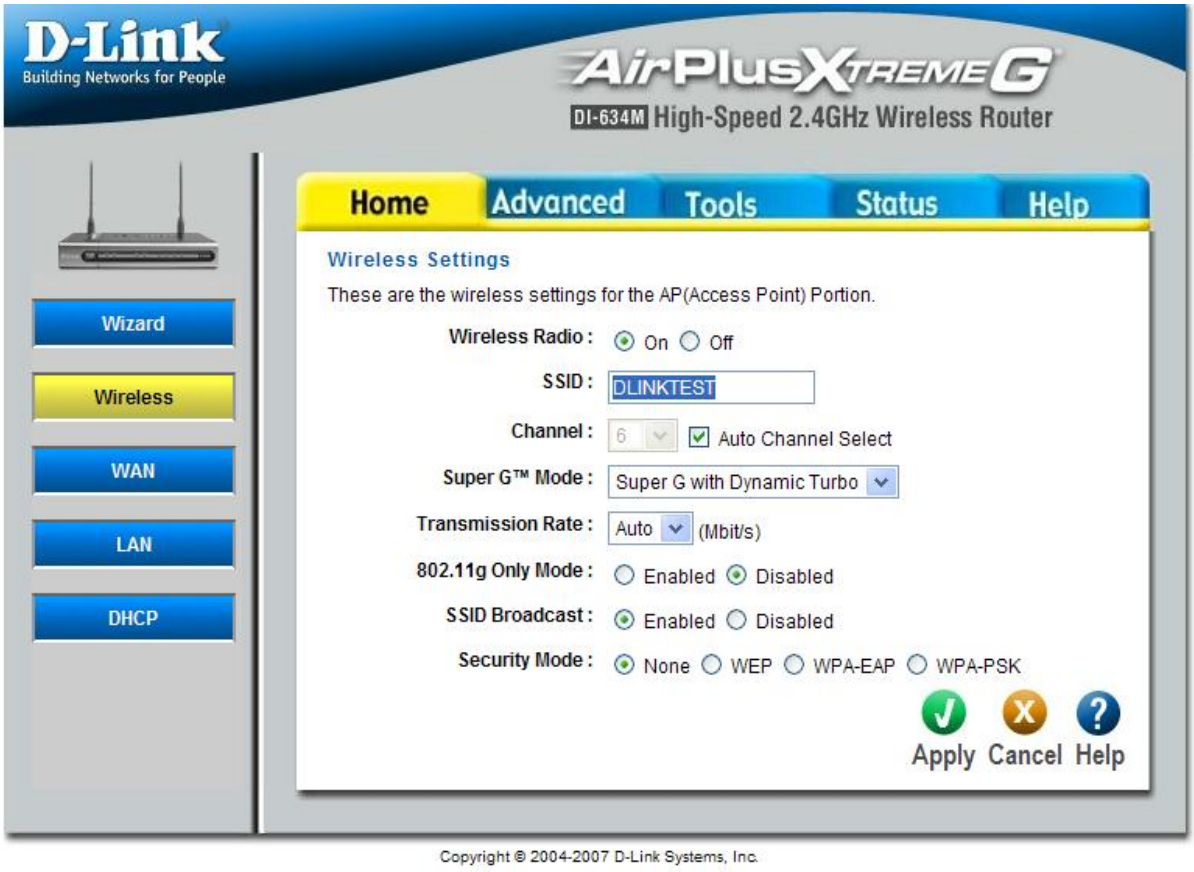


圖 3.2.3 Infrastructure 模式 網頁設定 SSID

4.點選 Home → WAN，然後點選 Clone Your PC's MAC Address 按鈕，以更新 PC 電腦的網卡位址(如~畫面中數字標示 1)。

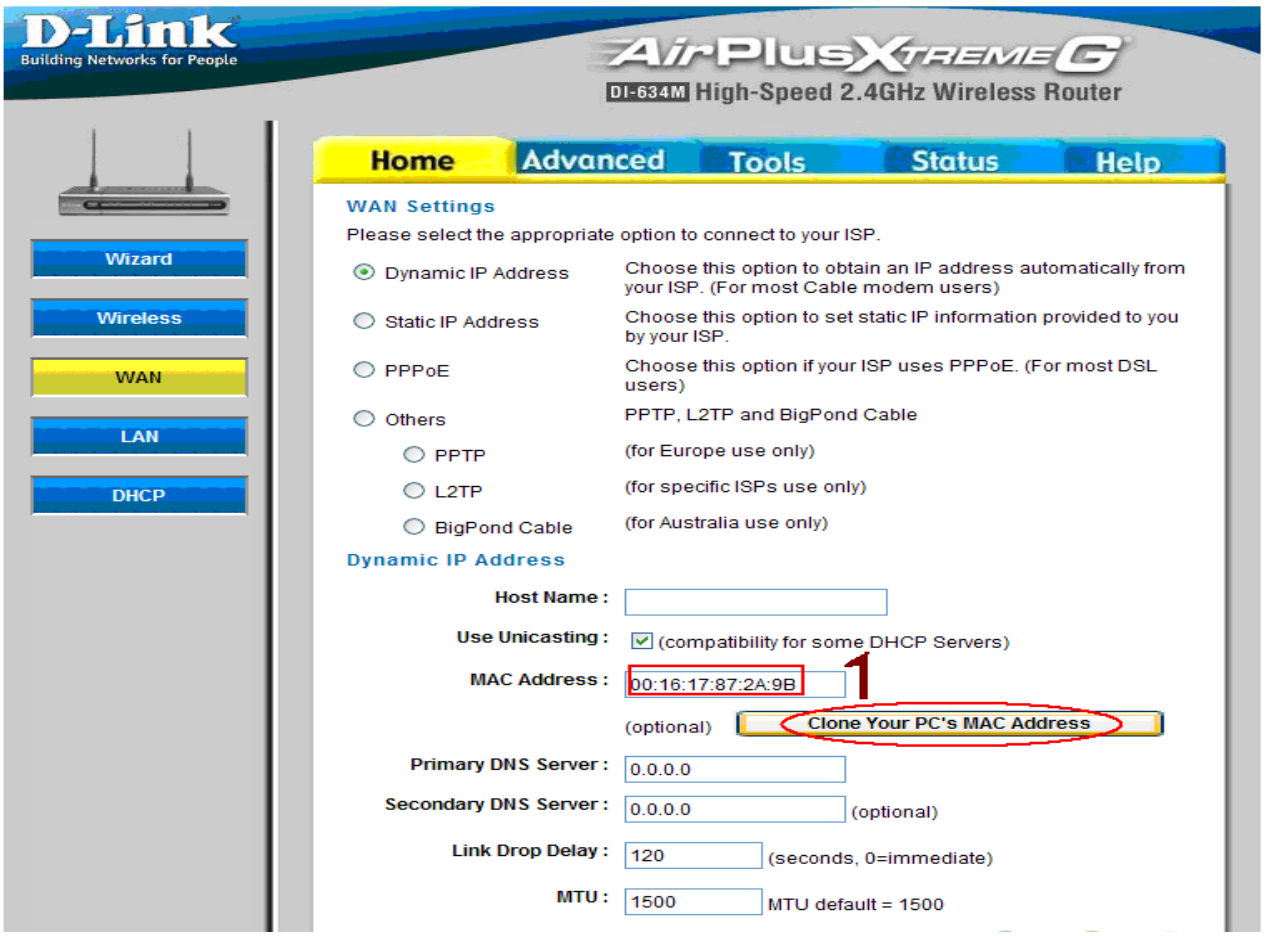


圖 3.2.4 Infrastructure 模式 網頁更新網卡位址

5.點選 Home → LAN，在這畫面的 IP Address 欄位就是輸入進入 AP 設定頁面所需 IP 位址(預設的 192.168.0.1，如果不喜歡就可以改成別的 IP 位址)，如下

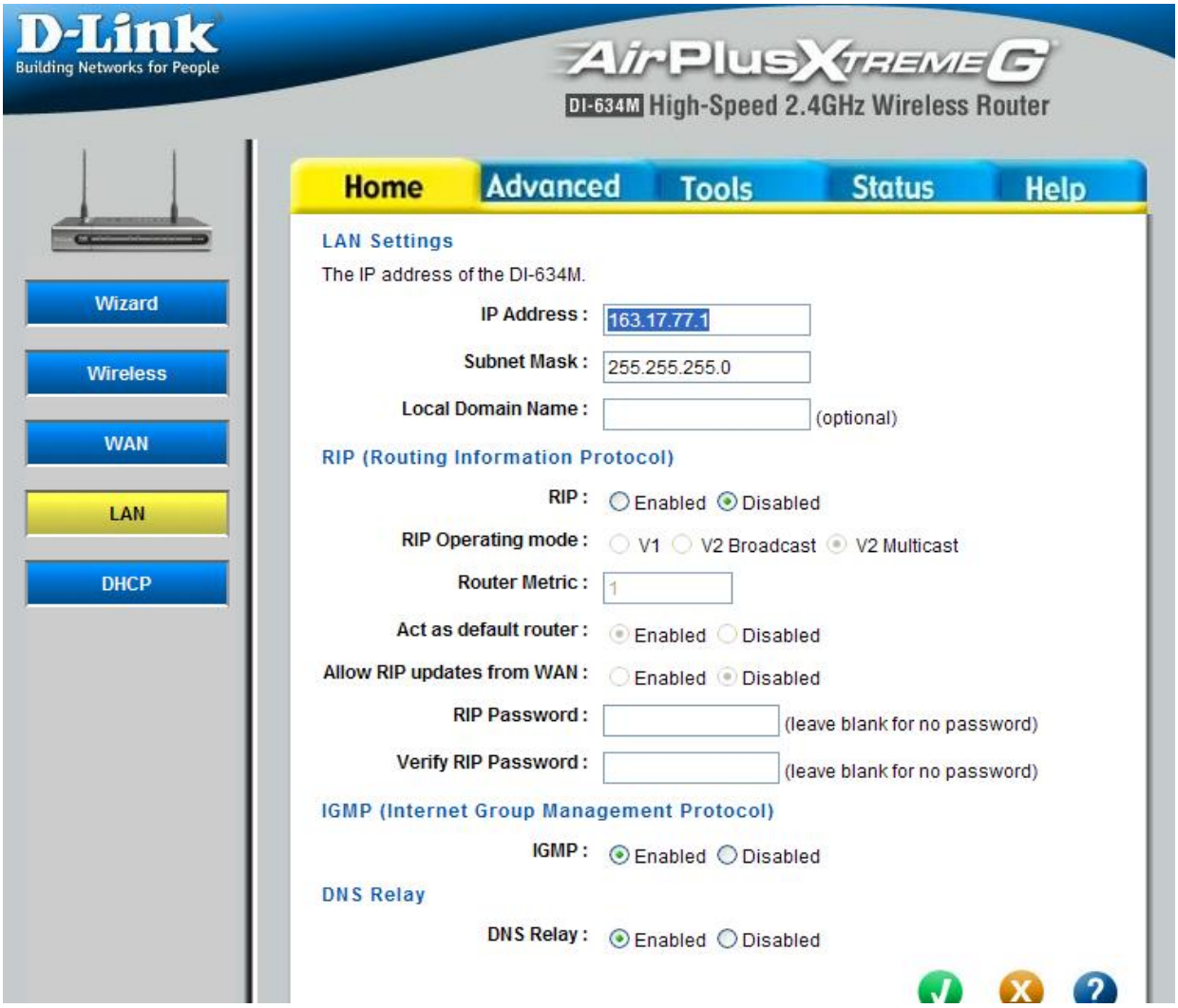


圖 3.2.5 Infrastructure 模式 網頁設定 AP 位址(IP Address)

6.點選 Home → DHCP，DHCP IP Address Range 欄位是用來輸入的 IP 位址的範圍，如下

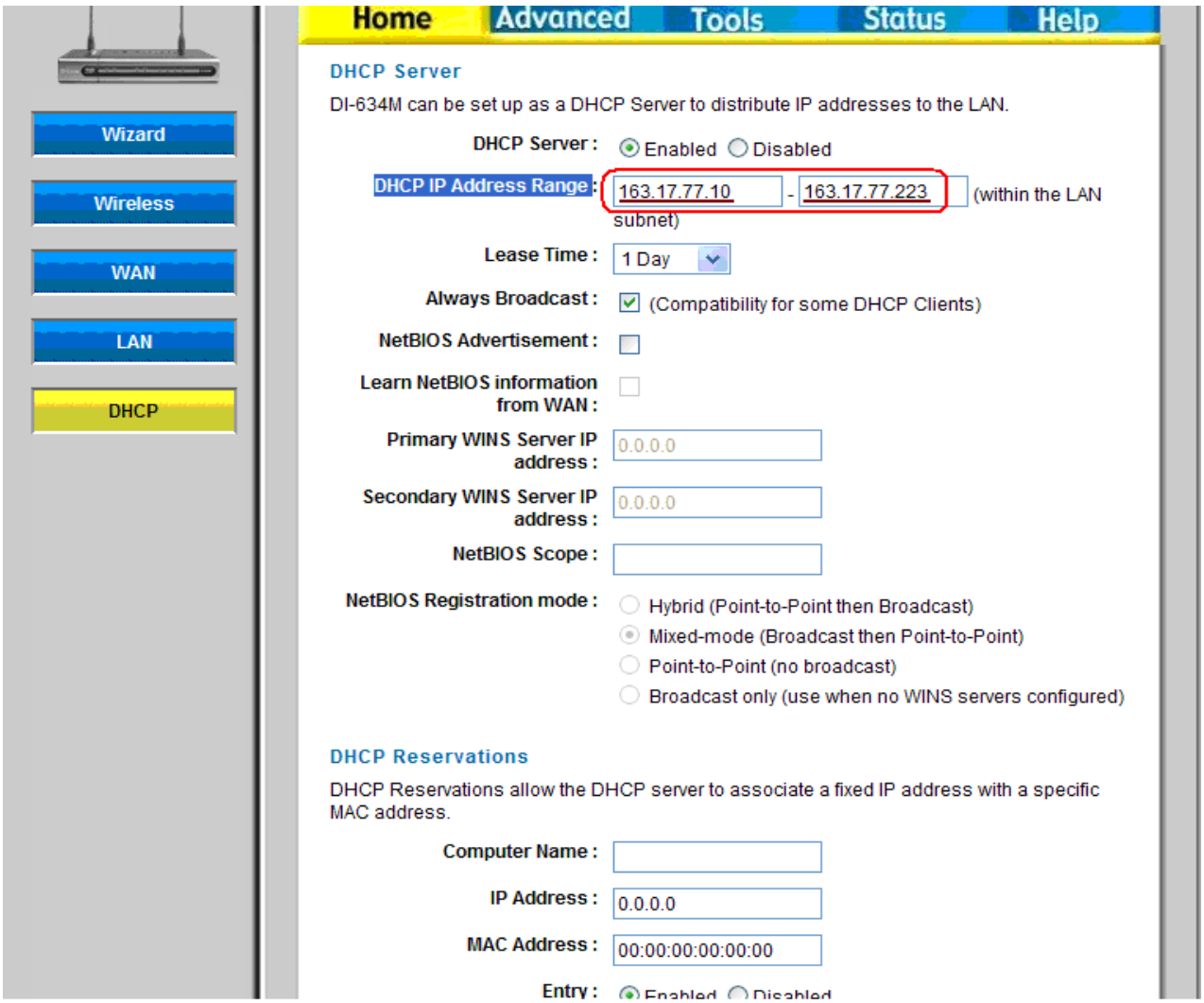


圖 3.2.6 Infrastructure 模式 網頁設定 IP 位址範圍

7.在左下角點開始→執行，再開啟欄位輸入 cmd 按確定，會跑出命令提示的視窗，在視窗中輸入 ipconfig /all，這指令是顯示本機位址和網卡編號一些的資訊(如~畫面中數字標示 1)，然後再輸入 ping 163.17.77.1(AP 的位址)，這指令是嘗試連結到 AP 無線橋接器看能不能互通(如~畫面中數字標示 2)。接著 ping 163.17.77.11(是電腦的 IP 位址)，這指令也是測試看看能不能和 PC 電腦的主機位址作互通的動作(如~畫面中數字標示 3)。

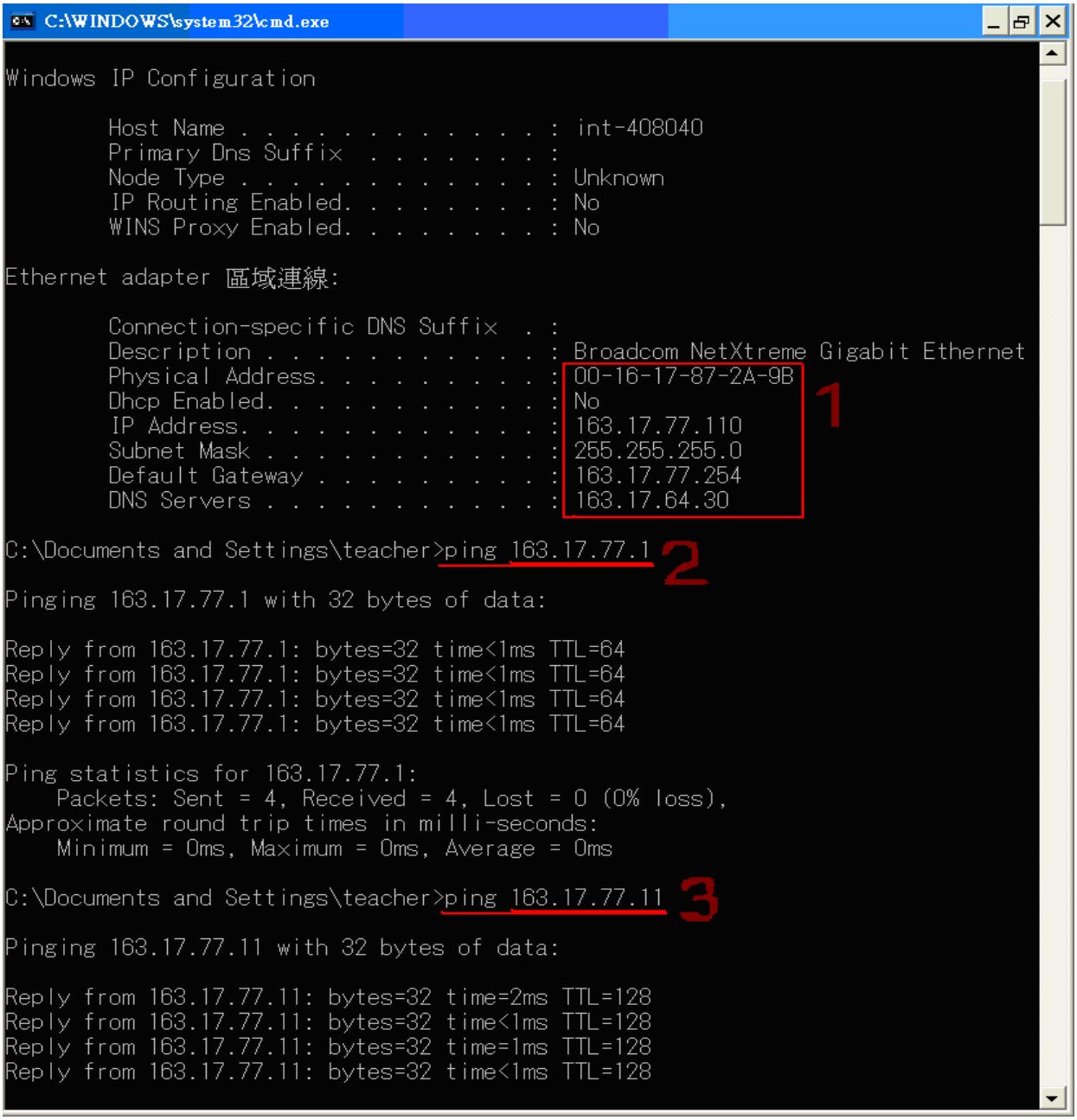


圖 3.2.7 Infrastructure 模式 命令提示視窗-PC 電腦

8.開啟我的電腦→網路上的芳鄰→搜尋→輸入您想找的電腦 IP 位址→點搜尋按鈕，如下

PC 電腦 →搜尋：163.17.77.11 →(NB 筆記型電腦的 IP 位址)

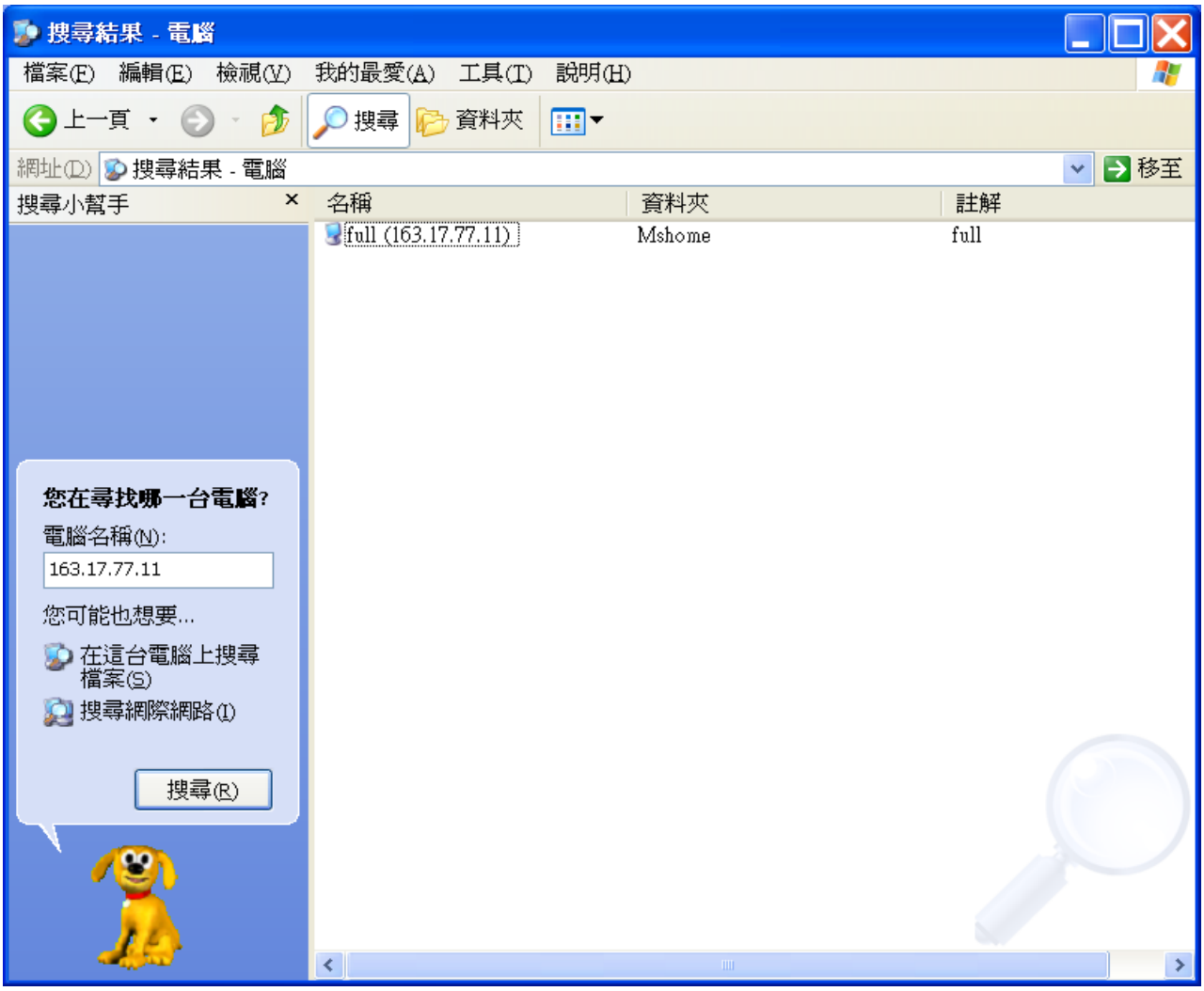


圖 3.2.8 Infrastructure 模式 搜尋結果-PC 電腦

9.互相做檔案共享的動作，以確認能互相連結的可行性。

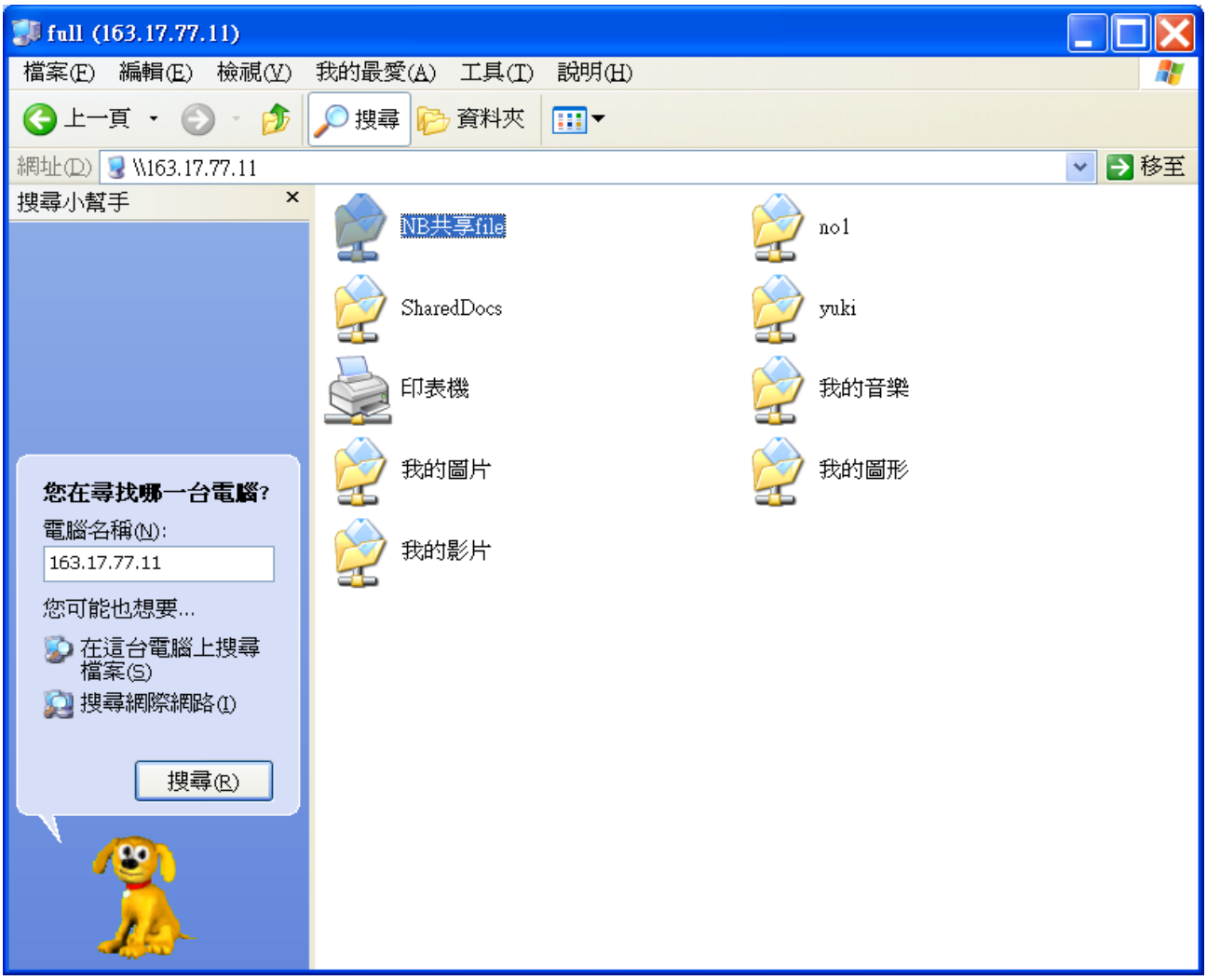


圖 3.2.9 Infrastructure 模式 檔案資料存取-PC 電腦

10.先安裝 Air Pcap 的驅動程式還有 WireShark 軟體，安裝完成之後，插入 Air Pcap 再開啟 WireShark，點選上面的選項 Capture，再選取 Interfaces 便會開啟下面圖示的視窗，選擇 AirPcap 網卡介面再點選 Options 作封包過濾。

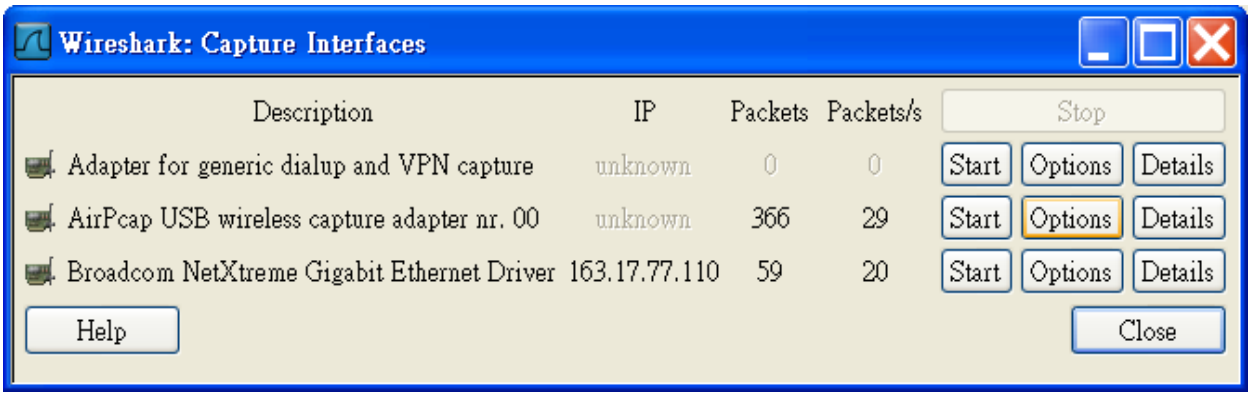


圖 3.2.10 Infrastructure 模式 封包擷取前的設定-PC 電腦

11.接著便會出現以下圖示的視窗，將 capture packets in promiscuous mode 選項不要打勾(如~畫面中數字標示 1)，再點選 capture filter:，以設定條件擷取 PC 電腦的封包(如~畫面中數字標示 2)。

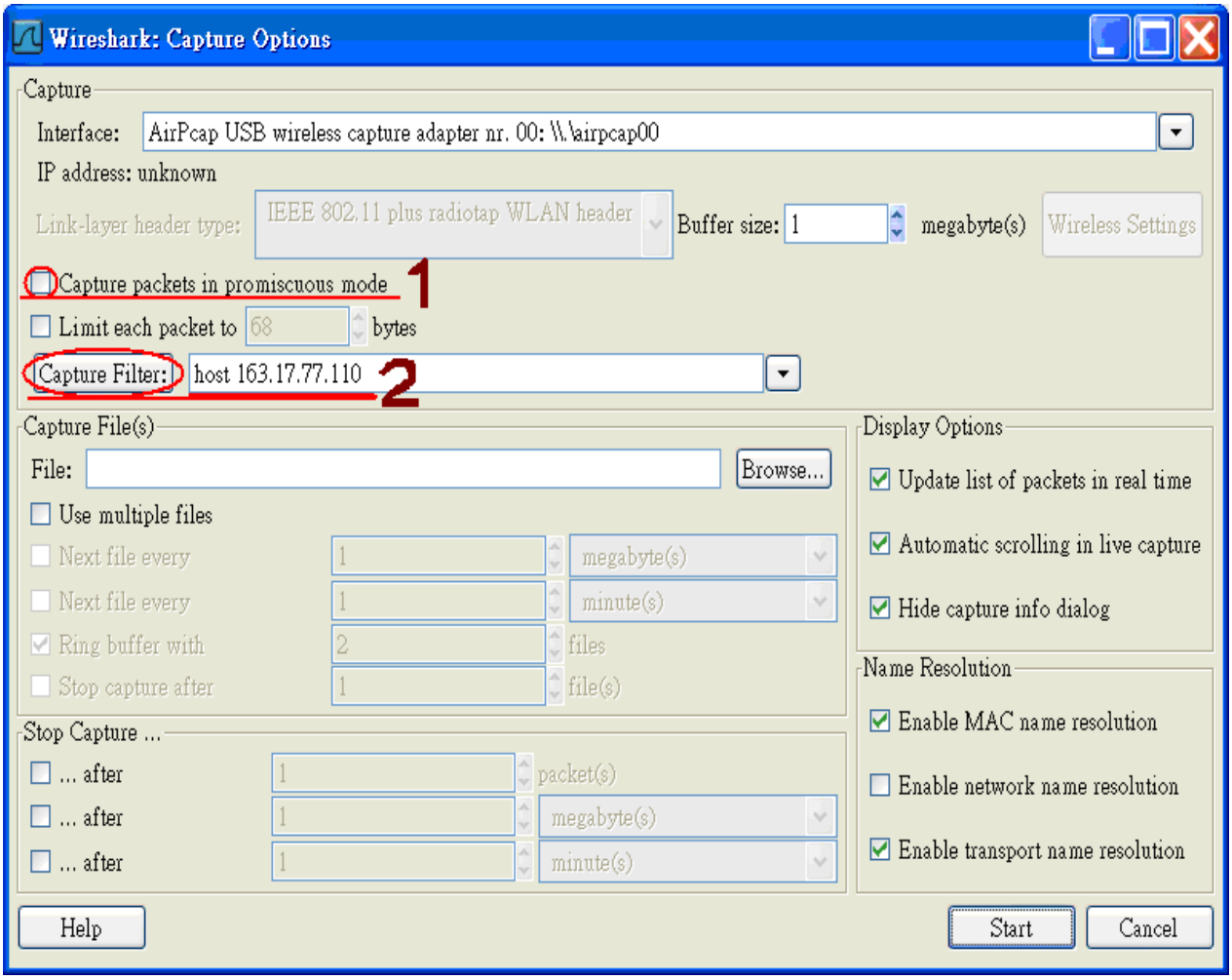


圖 3.2.11 Infrastructure 模式 封包擷取前的過濾-PC 電腦

12.利用上述的步驟，便能擷取到以下的封包內容，便是我們所必須解析的封包資訊。

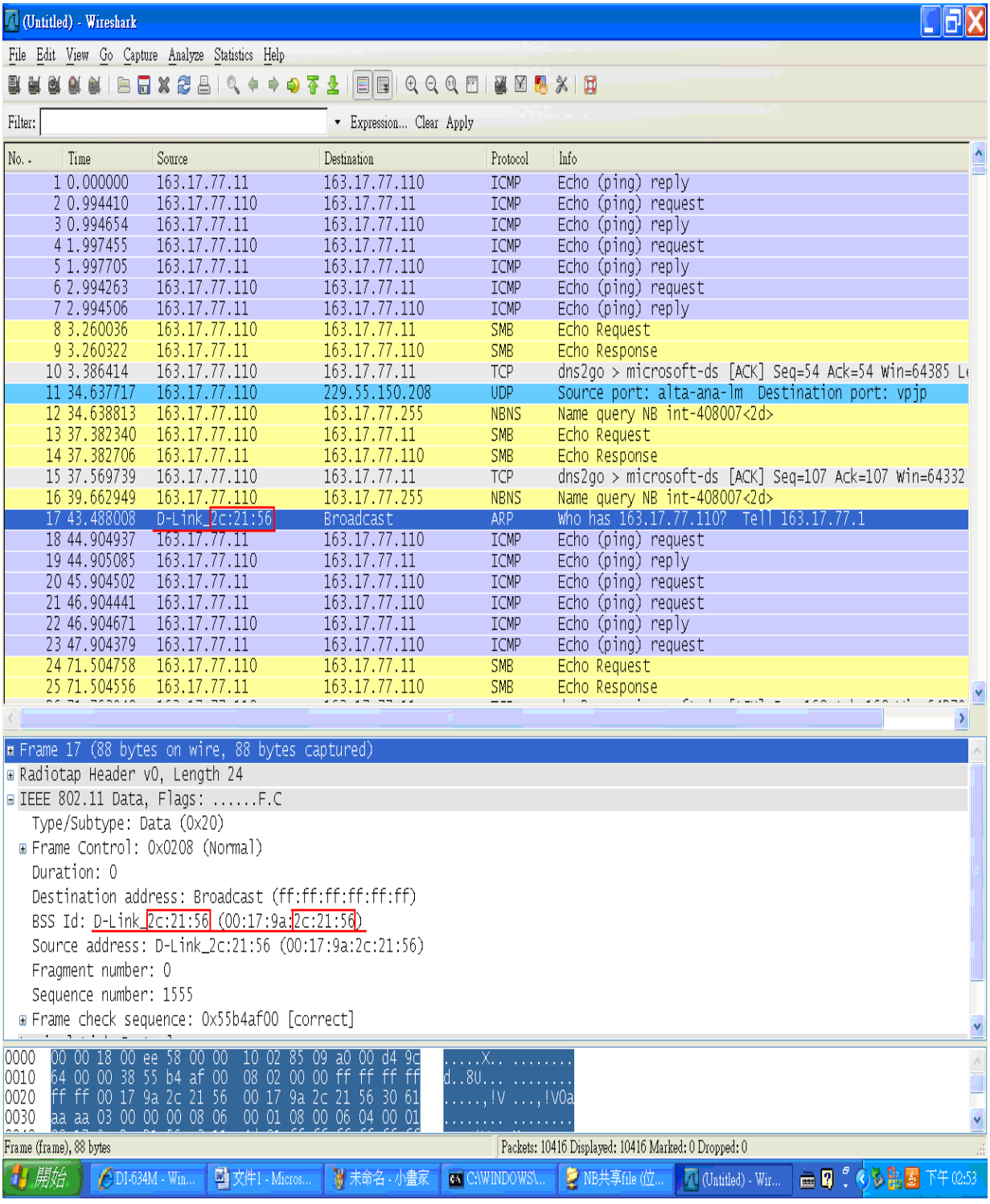


圖 3.2.12 Infrastructure 模式 封包擷取結果-PC 電腦

3.2.2 NB 設定模式

1.進入無線網路連線的內容，點選「TCP/IP 內容」開啟，將 Notebook(NB 筆記型電腦)的 IP 位址，設定與 D-Link(AP)網站中相同的網段，如下

NB 筆記型電腦 → IP 位址設定成：163.17.77.11

子網路遮罩設：255.255.255.0

預設閘道設：163.17.77.254

慣用 DNS 伺服器：163.17.64.30

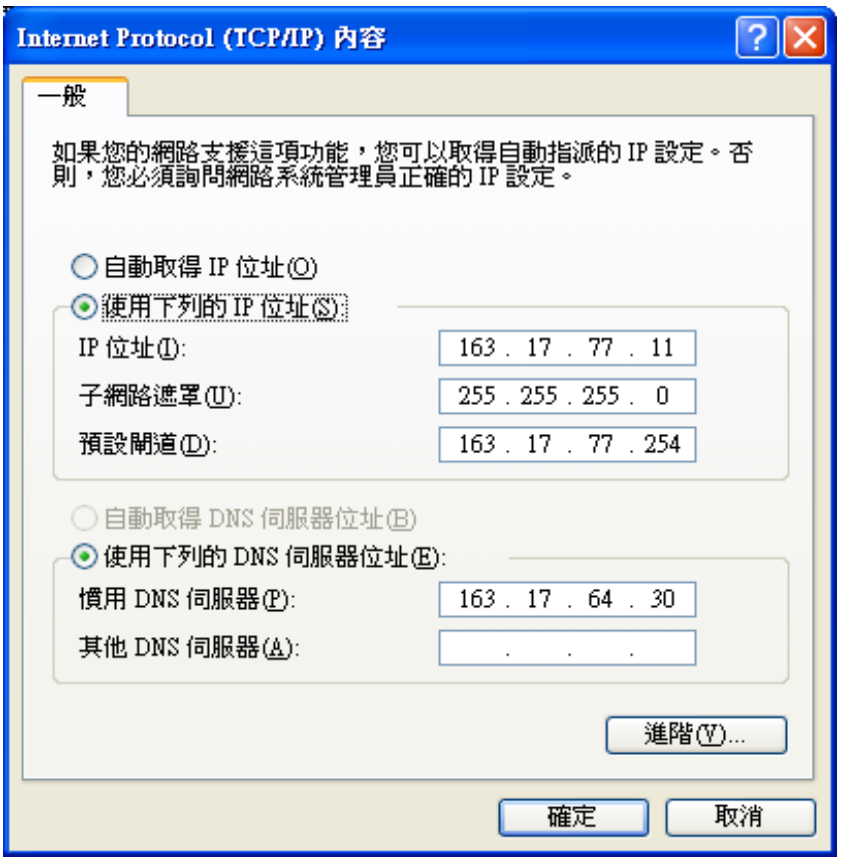


圖 3.2.12 Infrastructure 模式 IP 位址設定-NB 筆記型電腦

2.在視窗中點選上方的無線網路標籤，按「進階」鈕將網路設定成只給存取點的基礎結構模式

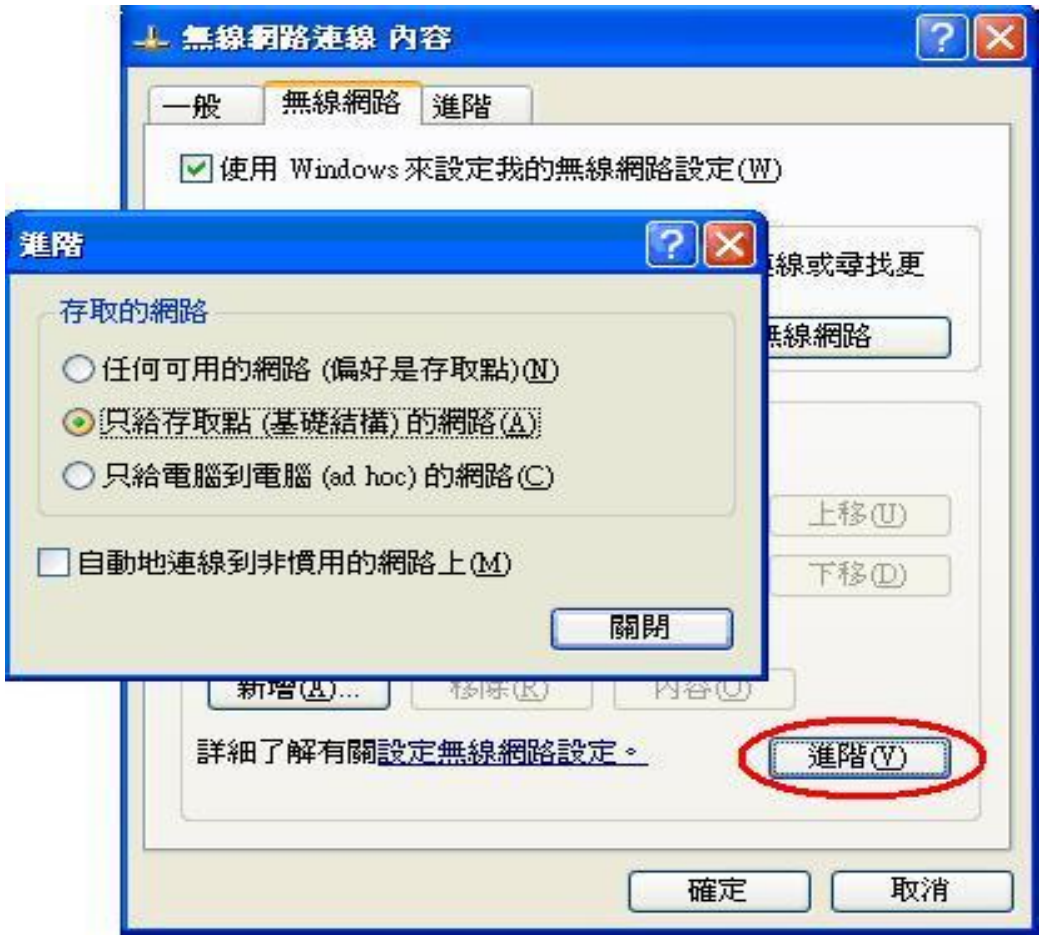


圖 3.2.13 Infrastructure 模式 存取的網路架構設定

3.將先前在 PC 電腦上設定的 SSID 名稱，點選該名稱 DLINKTEST(自動)，將「使用 Window 來設定我的無線網路設定」進行拘選後按確定鈕，如下圖

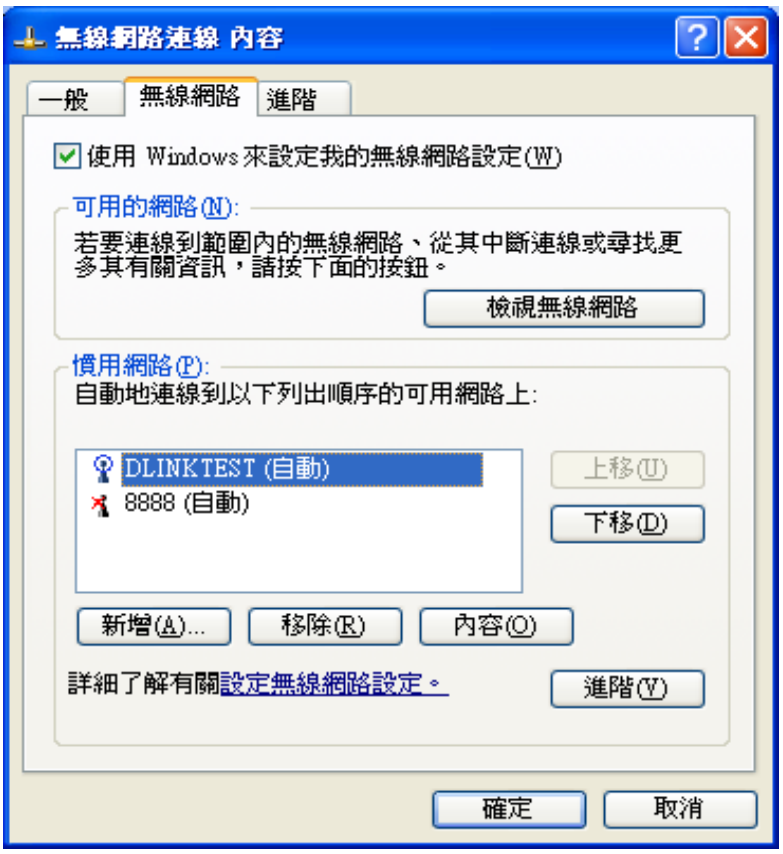


圖 3.2.14 Infrastructure 模式 已設定的 SSID 名稱

4.進入網路連線的視窗，在無線網路連線的圖示上按右鍵點選「檢視可用的無線網路」開啟視窗畫面，如下圖。 在視窗左方點選重新整理網路清單，等待先前設定的 SSID 名稱（DLINKTEST）出現在清單後，點選 DLINKTEST 進行連線。

圖 3.2.15 Infrastructure 模式 「無線網路連線」視窗

5.進入桌面工作列開始→執行的視窗，輸入 cmd 指令開啟命令提示畫面，使用關鍵字 ipconfig 的指令顯示出先前 NB 筆記型電腦設定的 IP 位址相關訊息，並使用關鍵字 ping 的指令檢查是否與 PC 電腦、AP 接通了，如下

指令：ipconfig →秀出先前在 NB 筆記型電腦上設定的 IP 位址 (如~畫面中的數字標示 1)

ping 163.17.77.1 →(網站上設定 AP 的 IP 位址，如~畫面中的數字標示 2)

ping 192.168.0.22 →(另一台 PC 電腦的 IP 位址，如~畫面中的數字標示 3)

由關鍵字 ping 的執行結果可看出 NB 筆記型電腦順利的與 PC 電腦、AP 接通了！

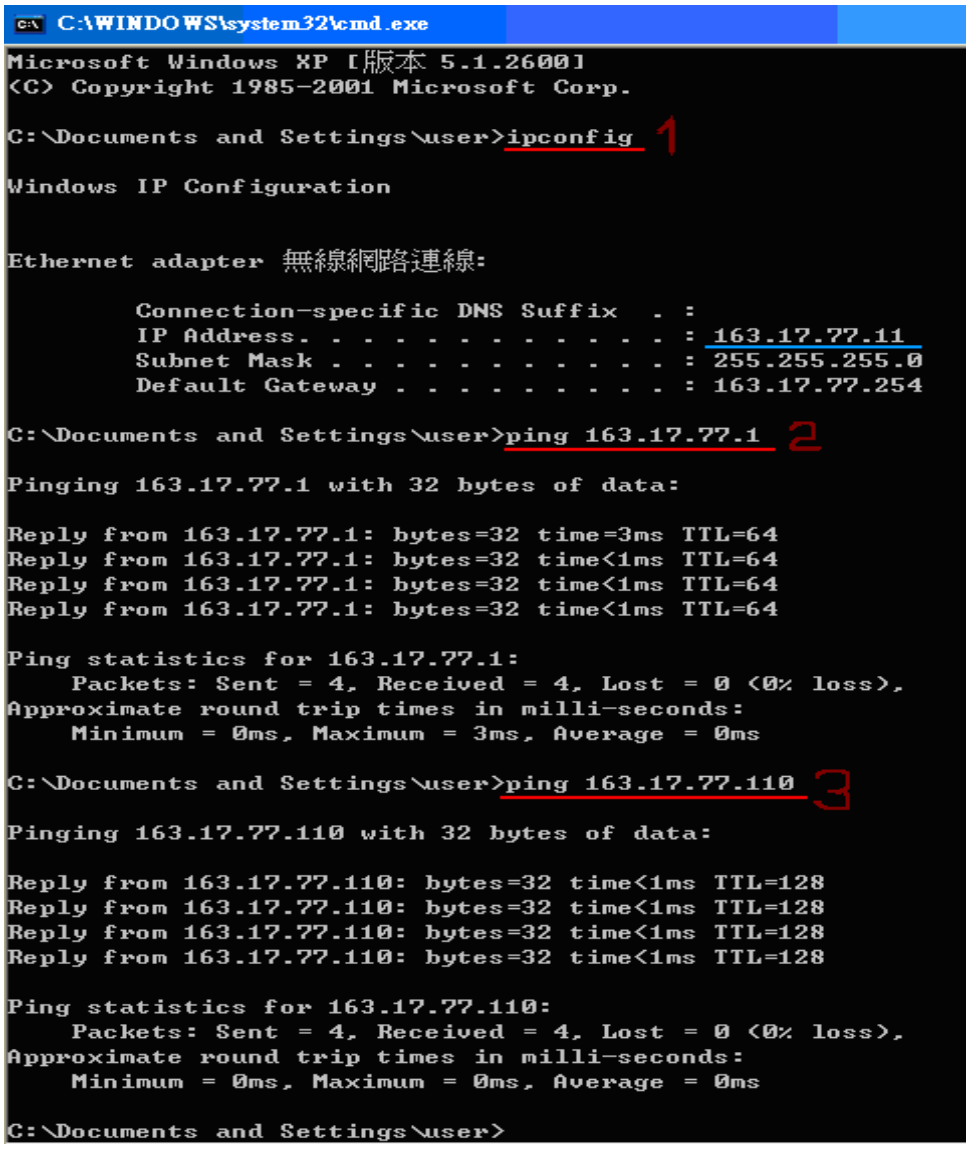


圖 3.2.16 Infrastructure 模式 命令提示視窗-NB 筆記型電腦

6.在 NB 筆記型電腦中點選資料夾，設定成共用模式，將檔案資料提供給另一台 PC 電腦存取使用，如下

7.進入網路上的芳鄰在左方電腦名稱，輸入 PC 電腦的 IP 位址，進行搜尋存取檔案資料，如下

NB 筆記型電腦 → 搜尋：163.17.77.110 →(PC 電腦的 IP 位址)

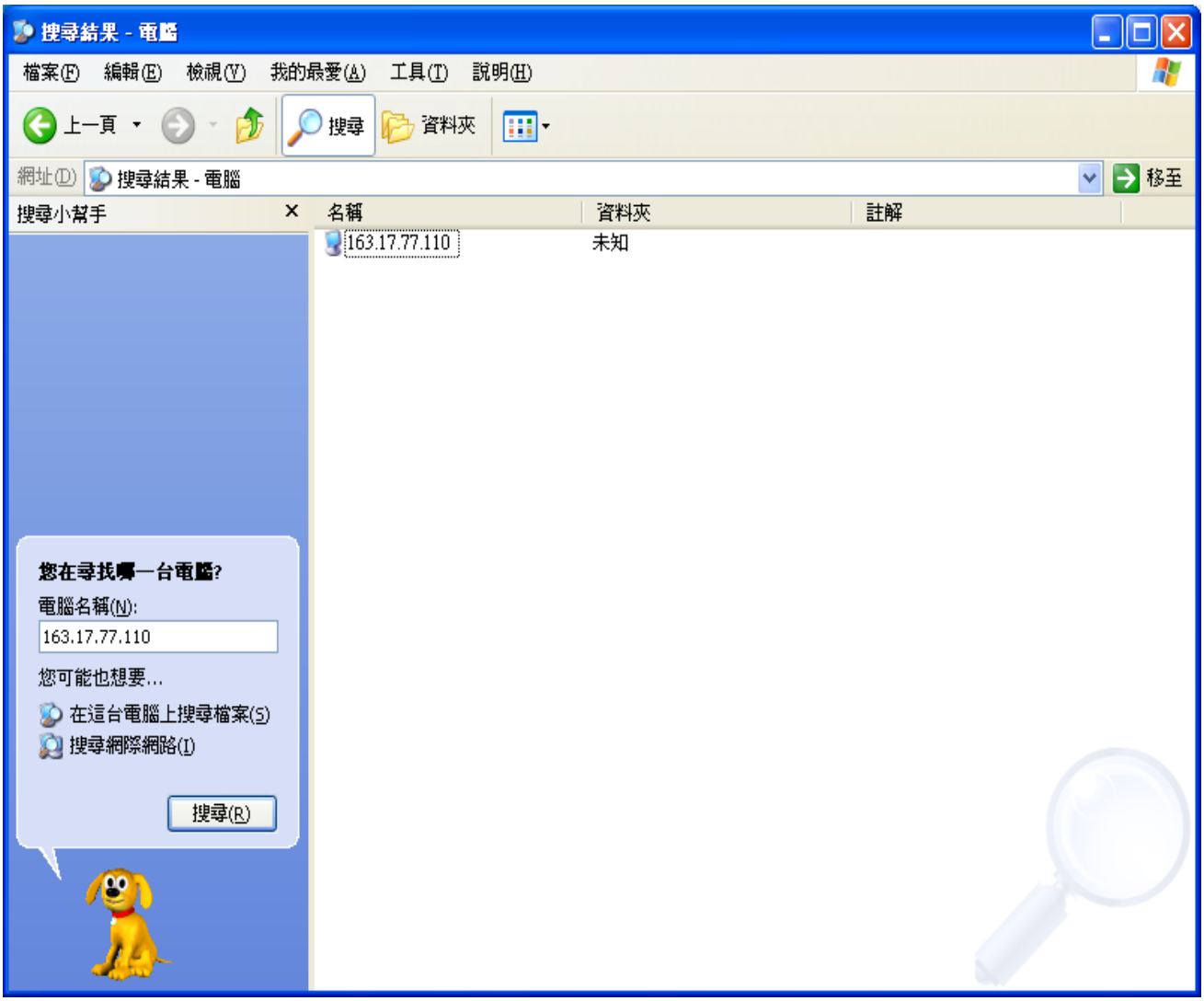


圖 3.2.17 Infrastructure 模式 搜尋結果-NB 筆記型電腦

8.進入 WireShark 封包擷取軟體，接上 USB 型式的外接式網卡 AirPacp，點選上方 Capture→ 開啟 Interfaces 視窗畫面，選擇 AirPcap 網卡介面的 Options 按鈕開始作封包過濾設定。

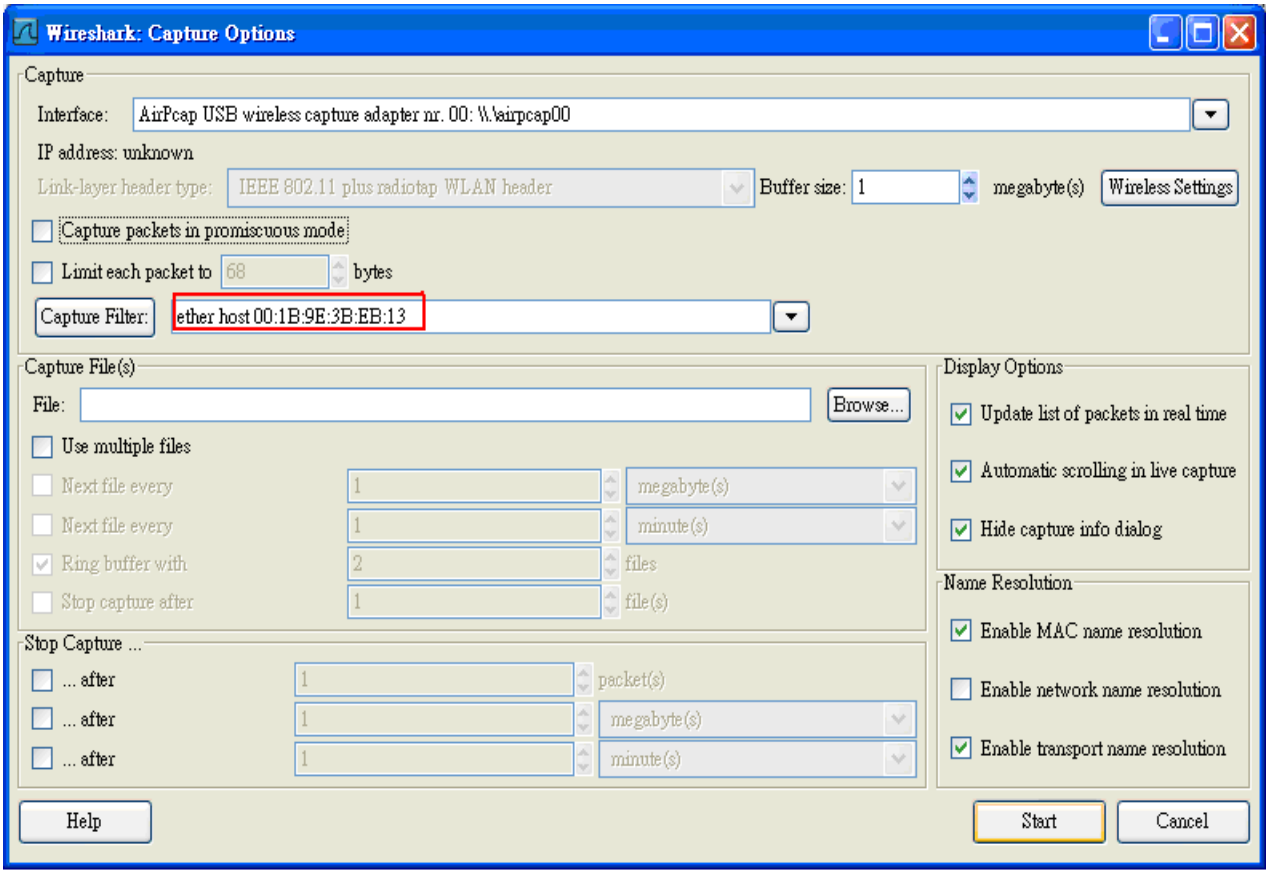


圖 3.2.18 Infrastructure 模式 封包擷取前的過濾-NB 筆記型電腦

9.在上半段的封包擷取畫面中，將會看見許多包含有自己和外界的封包，而從右方 Info 欄位訊息當中，即可判斷出來。 在下半段的封包資訊當中，將可在 IEEE 802.11 的展開畫面當中，看見 NB 筆記型電腦與 AP(D-Link)、PC 電腦互傳檔案時的 16 進位封包資料。

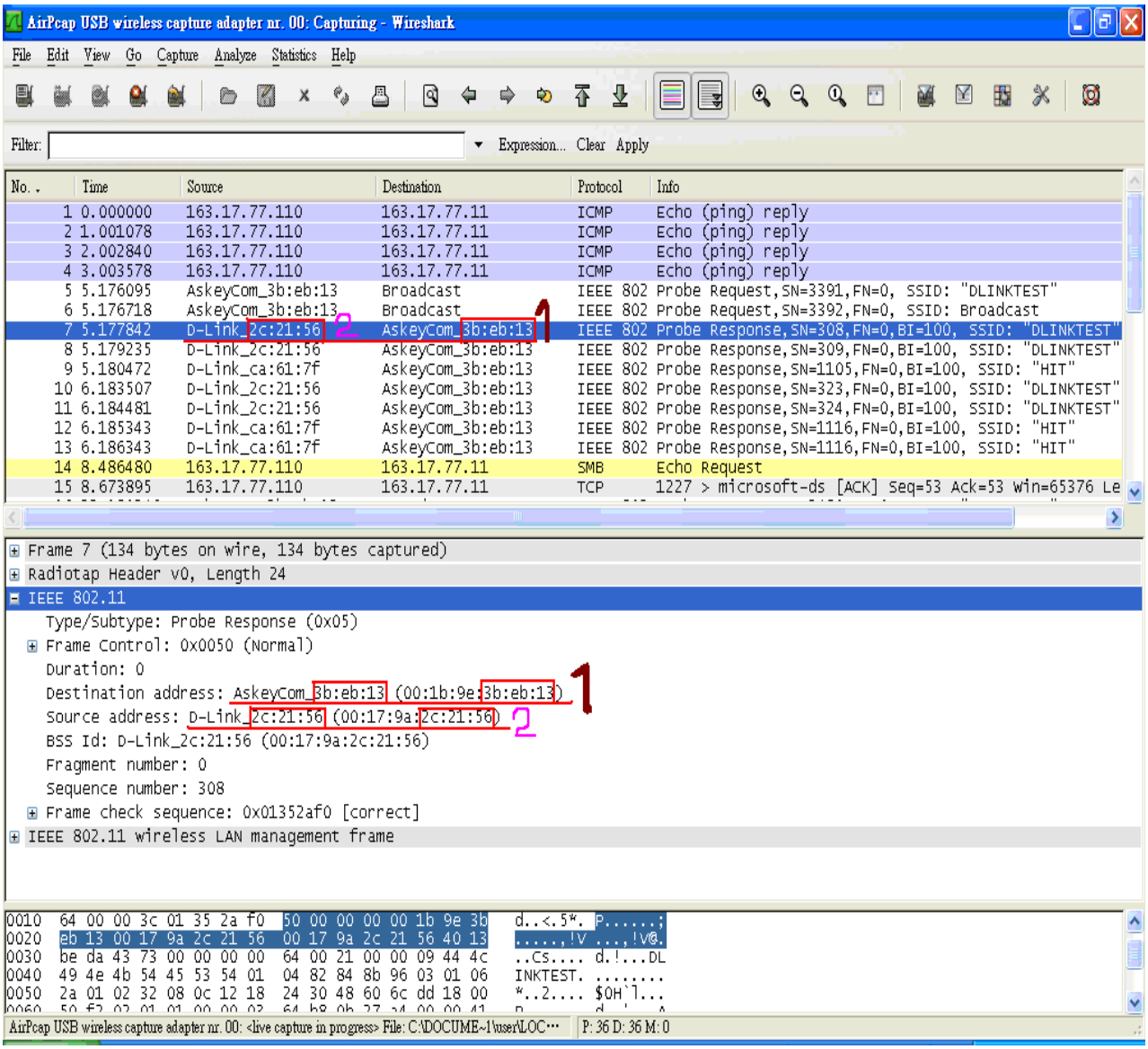
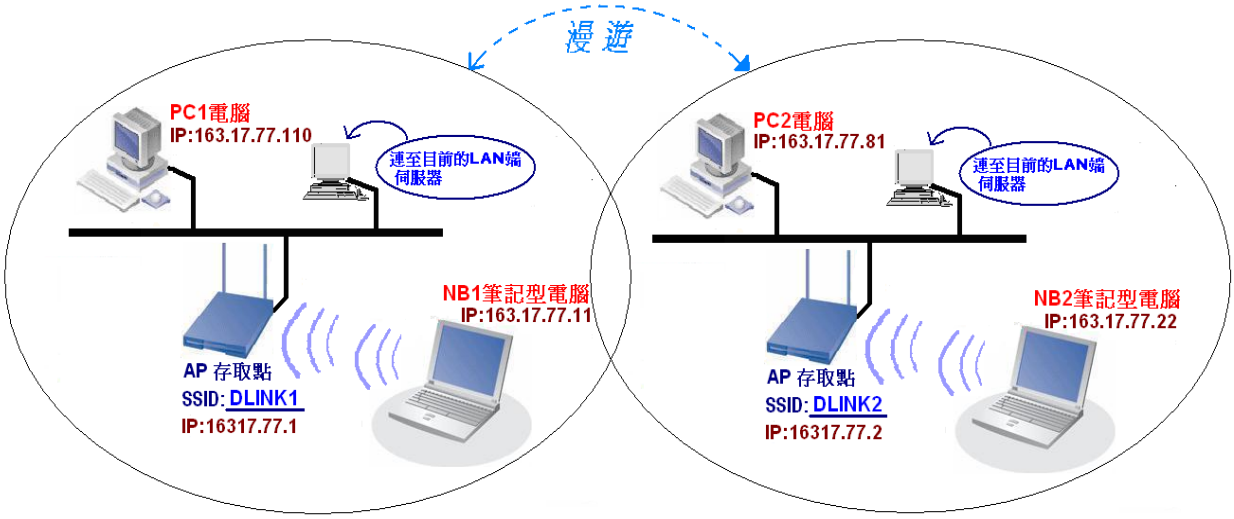


圖 3.2.19 Infrastructure 模式 封包擷取結果-NB 筆記型電腦

3.3 Infrastructure 模式-透過「2 台」AP 互連

3.3.1 「PC1 電腦←→D-Link 1(AP)←→NB1 筆記型電腦」的連接設定



Infrastructure 無線網路模式(AP*2台)

1.進入 PC1 電腦的區域連線內容，點選「TCP/IP 內容」開啟，設定與 D-Link1(AP)網站中相同網段的 IP 位址，如下

PC1 電腦的 IP 位址

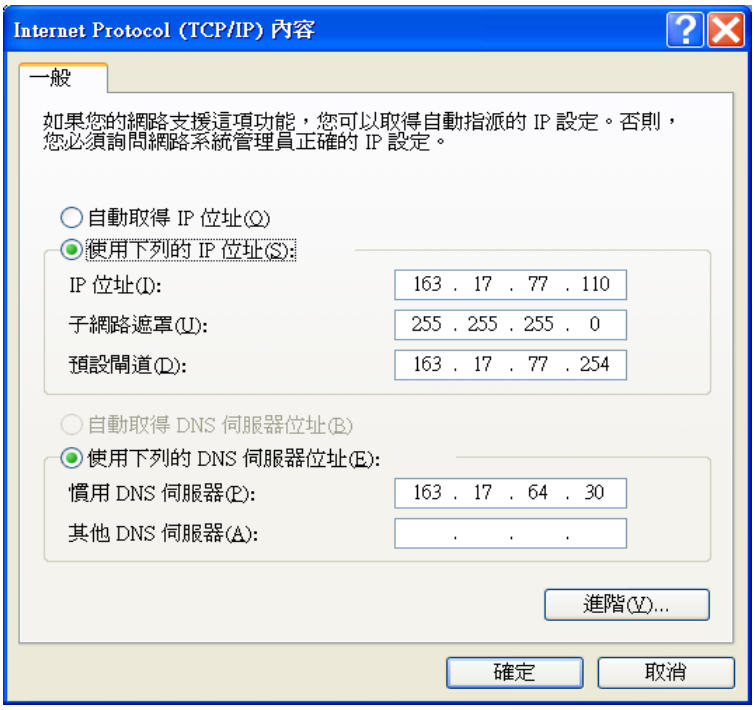


圖 3.3.1 Infrastructure(AP*2)架構 設定 PC1 電腦 IP 位址

2.進入 IE 瀏覽器在網址列輸入 192.168.0.1(預設)，開啟網頁進入 D-Link 的設定畫面，點選左方的 LAN 按扭，在 IP Address 欄位設定 AP 相同的網段，如下

D-Link AP 的同網段設定 → IP Address：163.17.77.1 →(如~畫面中的數字標示 1)

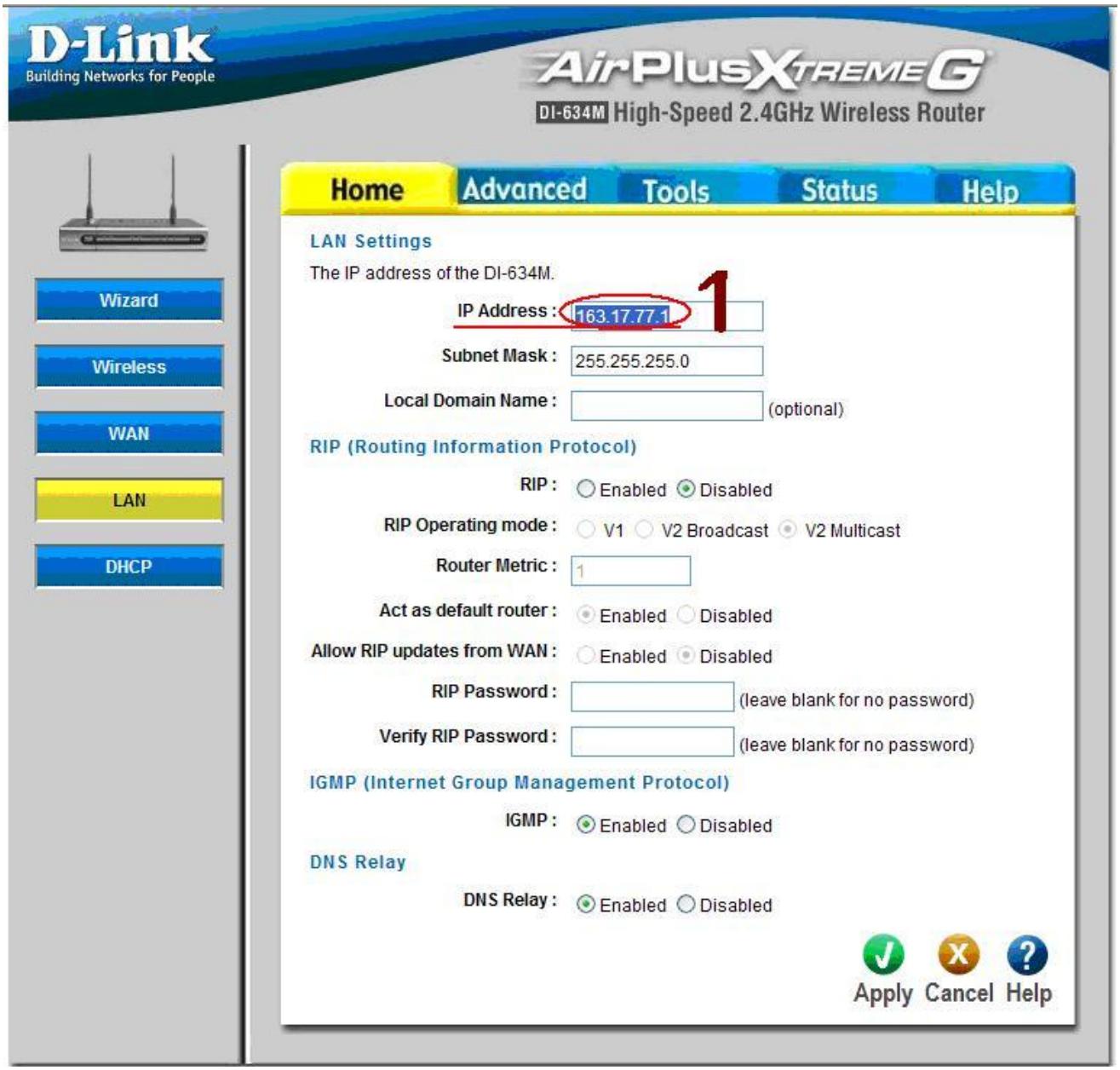


圖 3.3.2 Infrastructure(AP*2)架構 AP 位址設定頁面(IP Address)

3.在設定畫面點選左方的 Wireless 按鈕，進行 SSID 欄位的名稱輸入，如下

設定 D-Link 的 SSID 為 DLINK1(如~畫面中的數字標示 1)

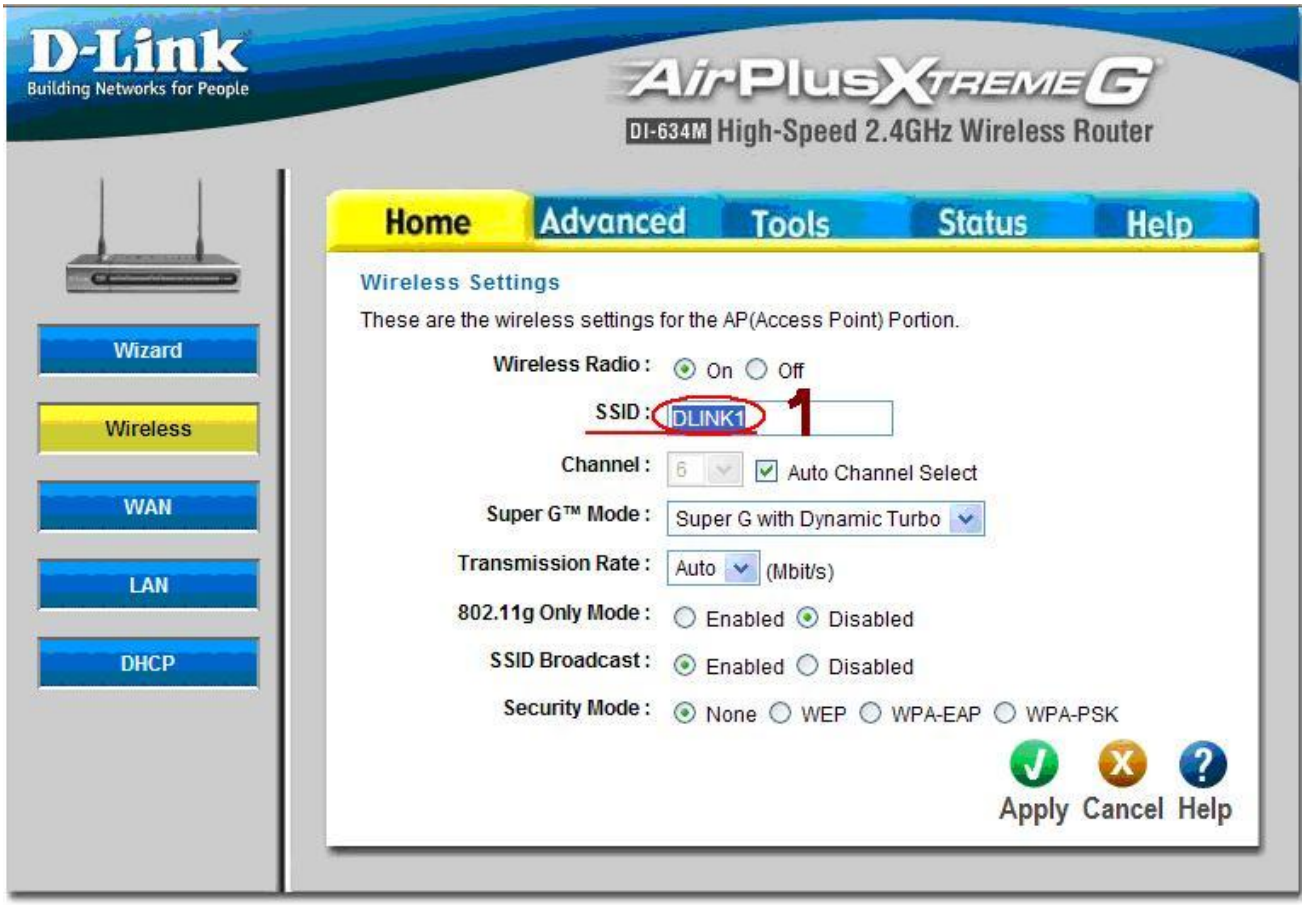


圖 3.3.3 Infrastructure(AP*2)架構 SSID 設定頁面

4.在設定畫面點選左方的 WAN 按鈕，再點選 Clone Your PC's MAC Address 按鈕，以更新 PC1 電腦的網卡位址(如~畫面中數字標示 1)。

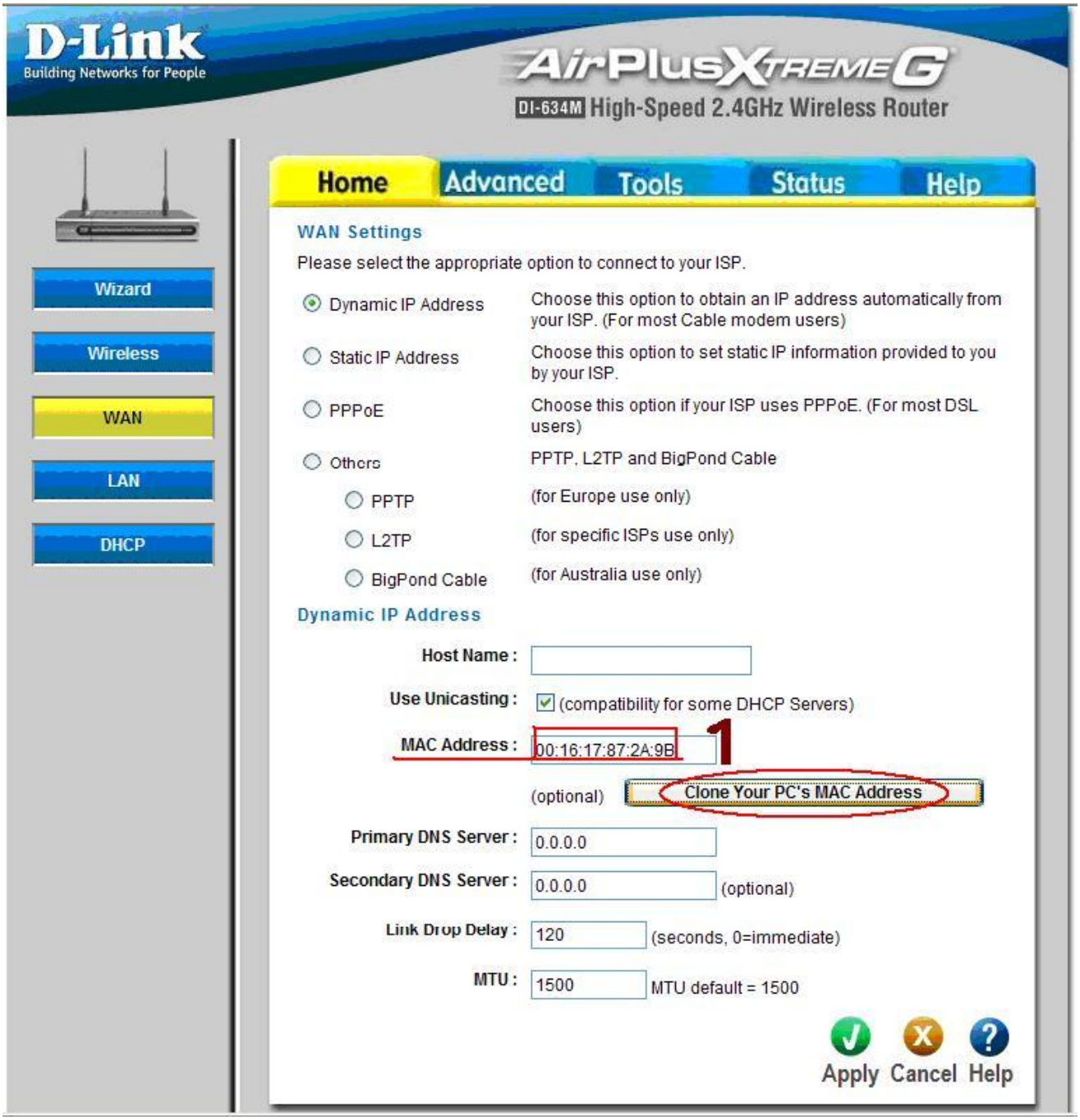


圖 3.3.4 Infrastructure(AP*2)架構 網卡位址更新設定

5.在設定畫面點選左方的 DHCP 按鈕，進行 DHCP IP Address Range 欄位的位址設定(163.17.77.10 – 163.17.77.223)，如下

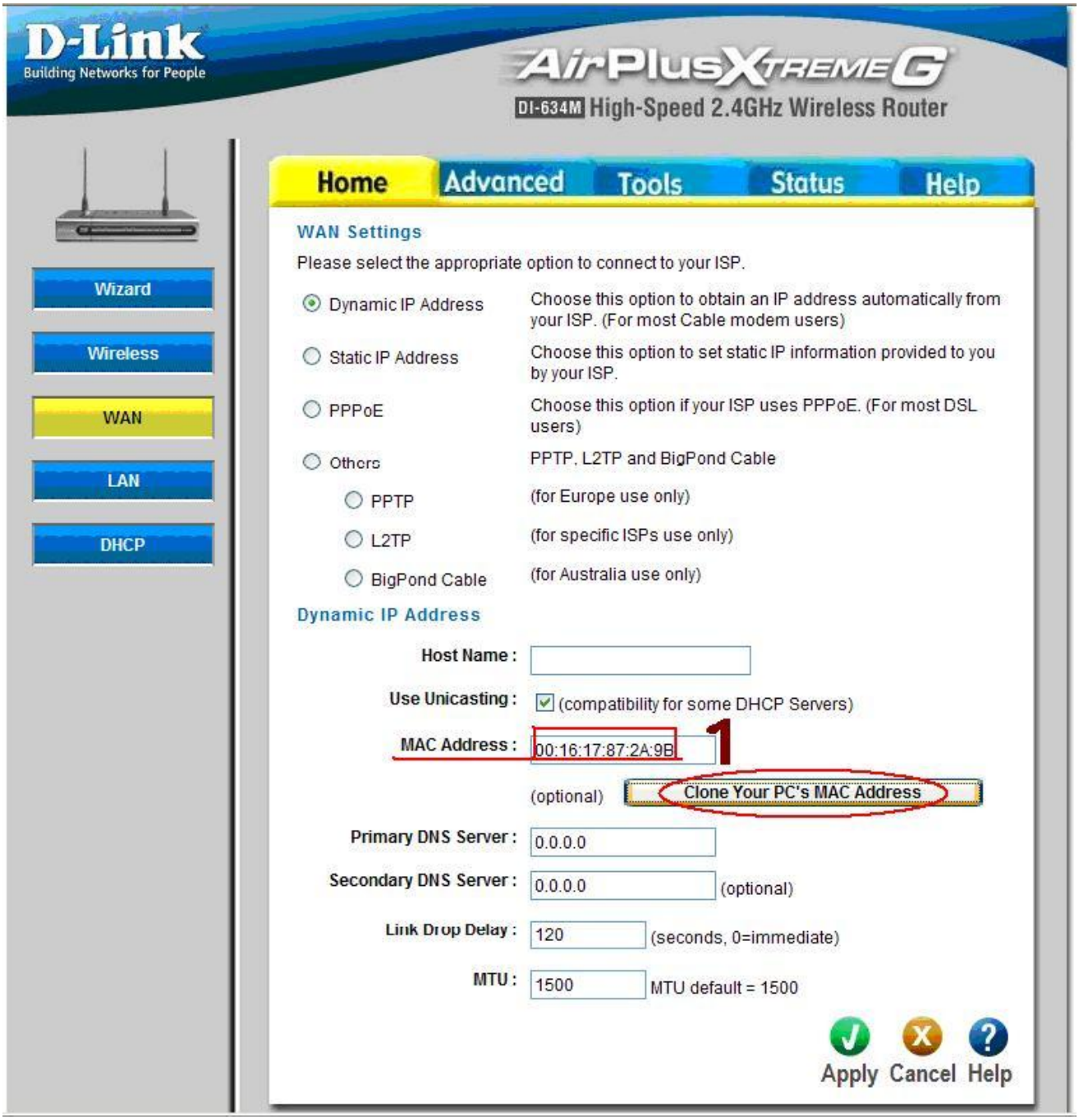


圖 3.3.5 Infrastructure(AP*2)架構 IP 位址範圍設定

6.進入桌面工作列開始 →執行的視窗，輸入 cmd 指令開啟命令提示畫面，使用關鍵字 ipconfig 的指令顯示出先前 PC1 電腦設定的 IP 位址相關訊息(如~畫面中的數字標示 1)，並使用關鍵字 ping 的指令測試 PC1 電腦跟 DLINK1(AP)是否互通(如~畫面中的數字標示 2)。

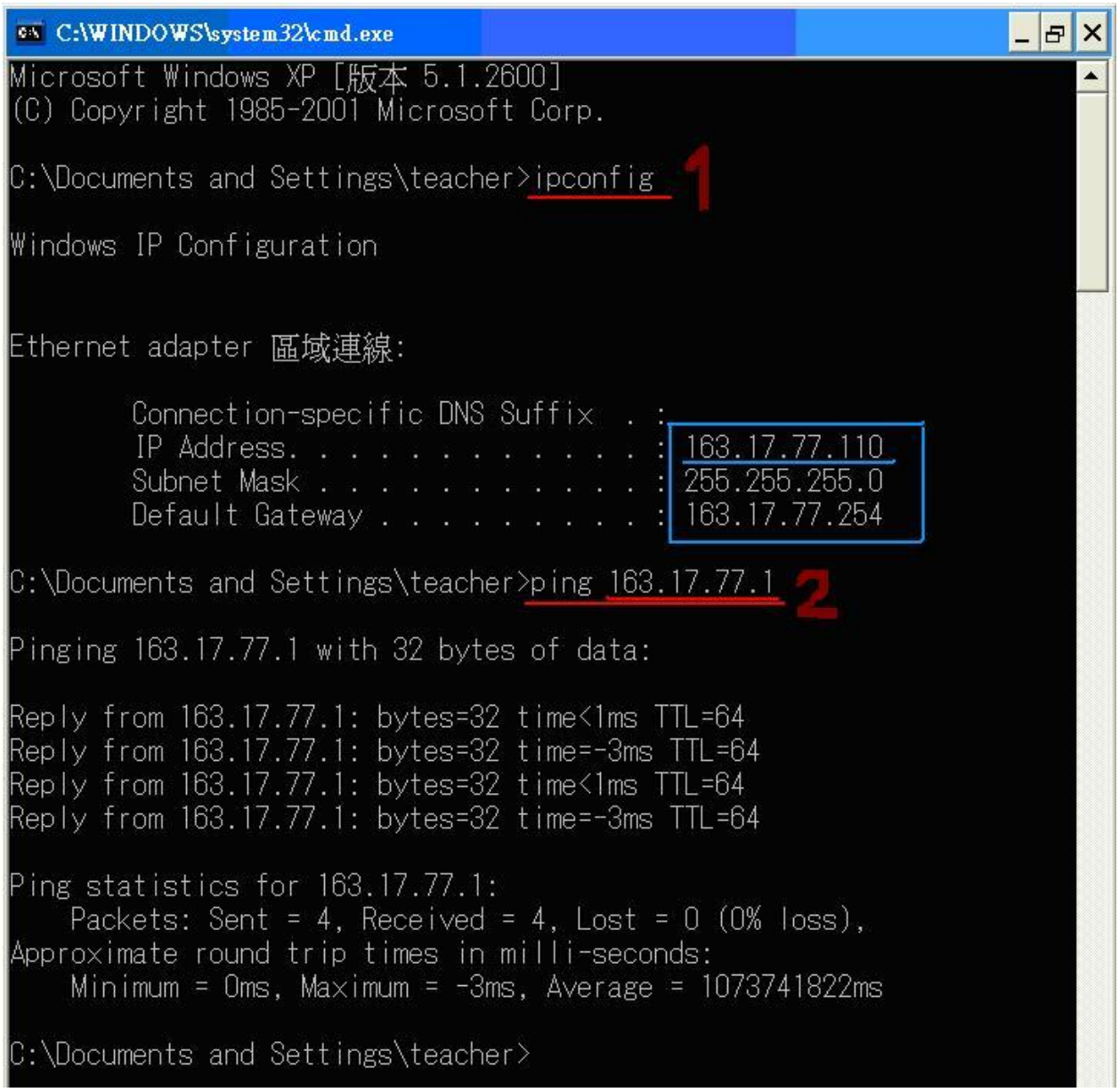


圖 3.3.6 Infrastructure(AP*2)架構 命令提示視窗操作-PC1 電腦

7.進入 NB1 筆記型電腦的無線網路連線內容，點選「TCP/IP 內容」開啟，設定與 D-Link1(AP)網站中相同網段的 IP 位址進行測試，如下

NB1 的 IP

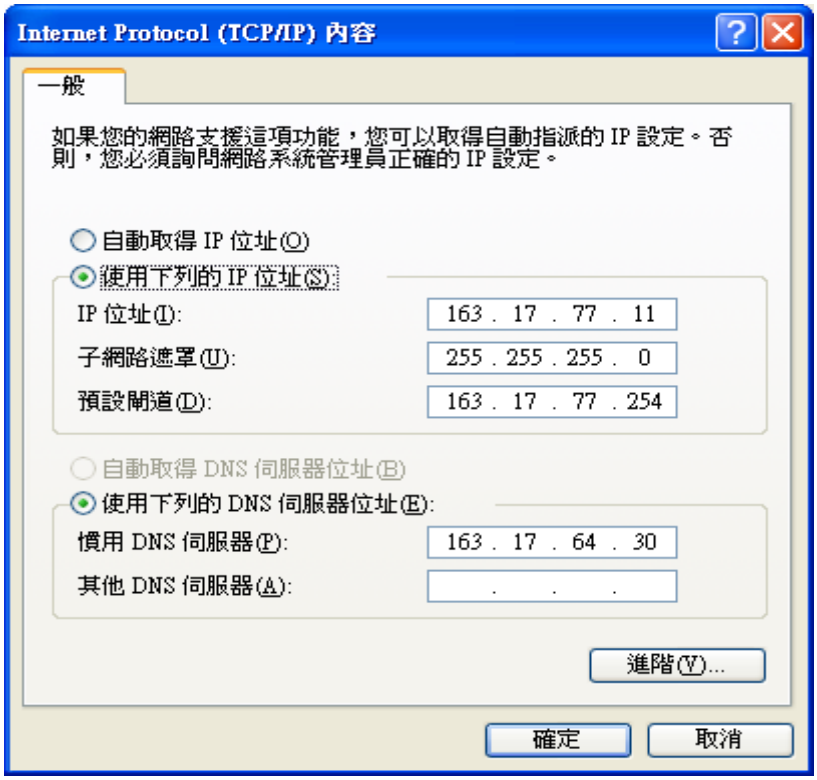


圖 3.3.7 Infrastructure(AP*2)架構 設定 NB1 筆記型電腦 IP 位址

8.進入網路連線的視窗，在無線網路連線的圖示上按右鍵點選「檢視可用的無線網路」開啟視窗畫面，如下圖。 在視窗左方點選重新整理網路清單，等待先前設定的 SSID 名稱（DLINK1）出現在清單後，會偵測自動連到 DLINK1。

圖 3.3.8 Infrastructure(AP*2)架構 「無線網路連線」視窗- NB1 筆記型電腦

9.進入桌面工作列開始 →執行的視窗，輸入 cmd 指令開啟命令提示畫面，使用關鍵字 ipconfig 的指令顯示出在 NB1 筆記型電腦所設定的 IP 位址(如~畫面中的數字標示 1)，並使用關鍵字 ping 的指令測試 NB1 是否可透過 DLINK1 連至 PC1 電腦跟它互通，如下

指令：ping 163.17.77.1 →網站上設定 DLINK1(AP)的 IP 位址(如~數字標示 2)

ping 192.168.0.110 →另一台 PC1 電腦的 IP 位址(如~數字標示 3)

由關鍵字 ping 的測試結果可知 NB1 筆記型電腦順利的透過 DLINK1 連至 PC1 電腦了。

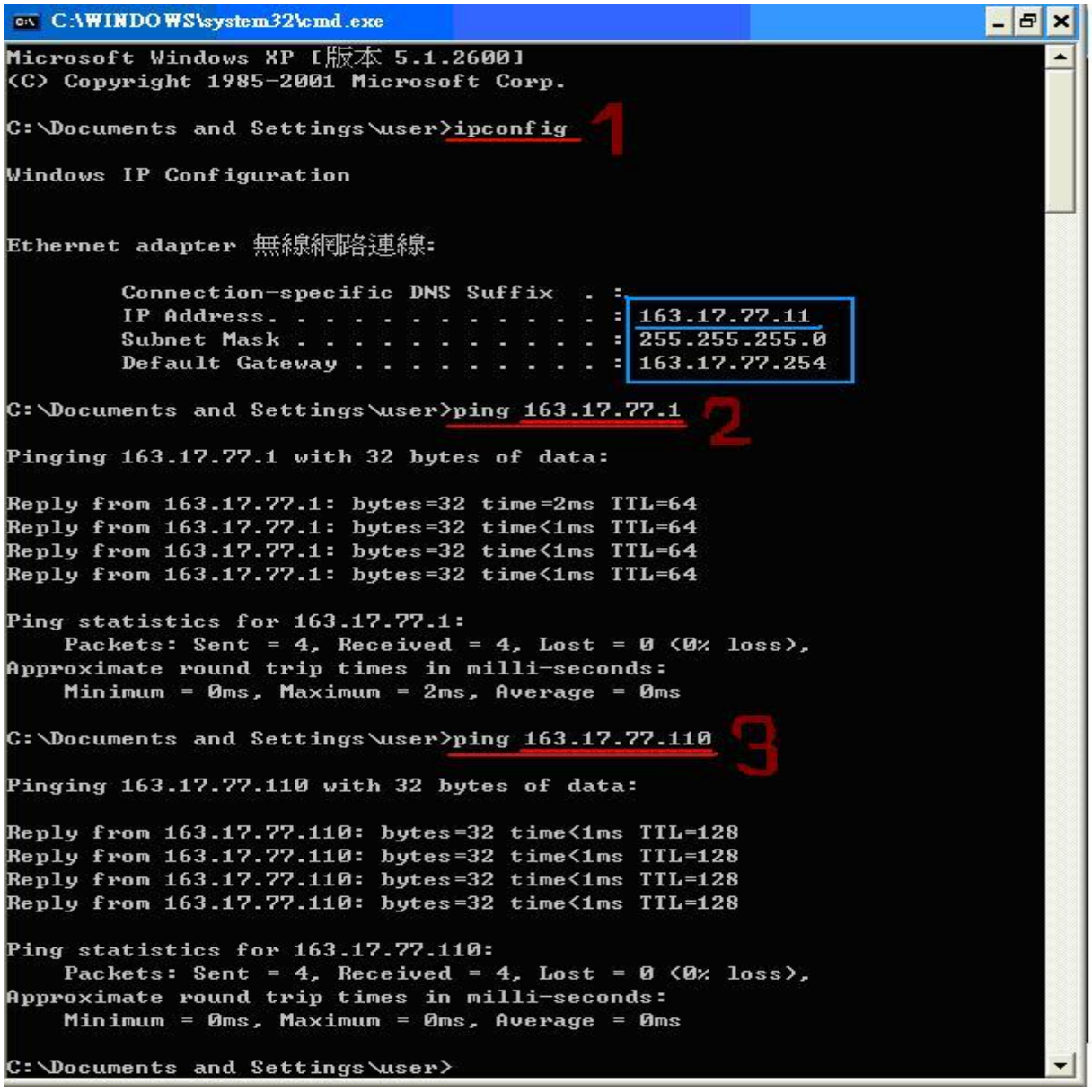


圖 3.3.9 Infrastructure(AP*2)架構 命令提示視窗操作- NB1 筆記型電腦

3.3.2 「PC2 電腦←→D-Link 2(AP)←→NB2 筆記型電腦」的連接設定

(按照上面相同的作法，設置另一小架構)

1.進入 PC2 電腦的區域連線內容，點選「TCP/IP 內容」開啟，設定與 D-Link2(AP)網站中相同網段的 IP 位址，如下

PC2 電腦的 IP 位址

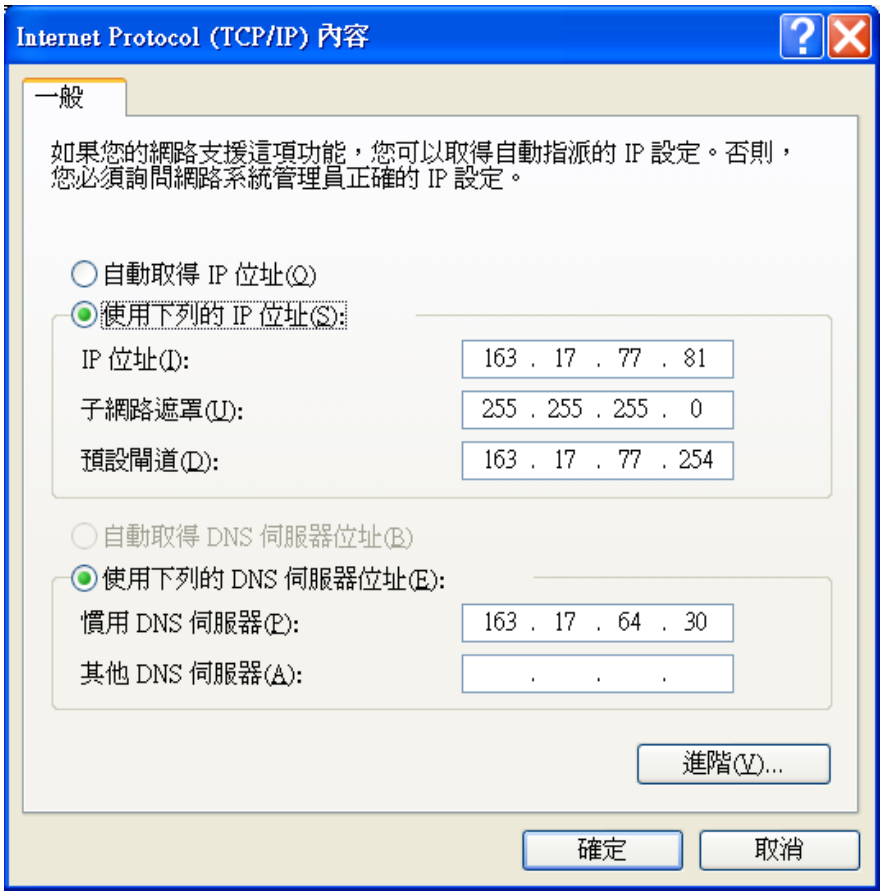


圖 3.3.10 Infrastructure(AP*2)架構 設定 PC2 電腦 IP 位址

2.進入 IE 瀏覽器在網址列輸入 192.168.0.1(預設)，開啟網頁進入 D-Link 的設定畫面，點選左方的 LAN 按扭，在 IP Address 欄位設定 AP 相同的網段，如下

DLINK2 的設定 → IP Address：163.17.77.2 →(如~畫面中的數字標示 1)

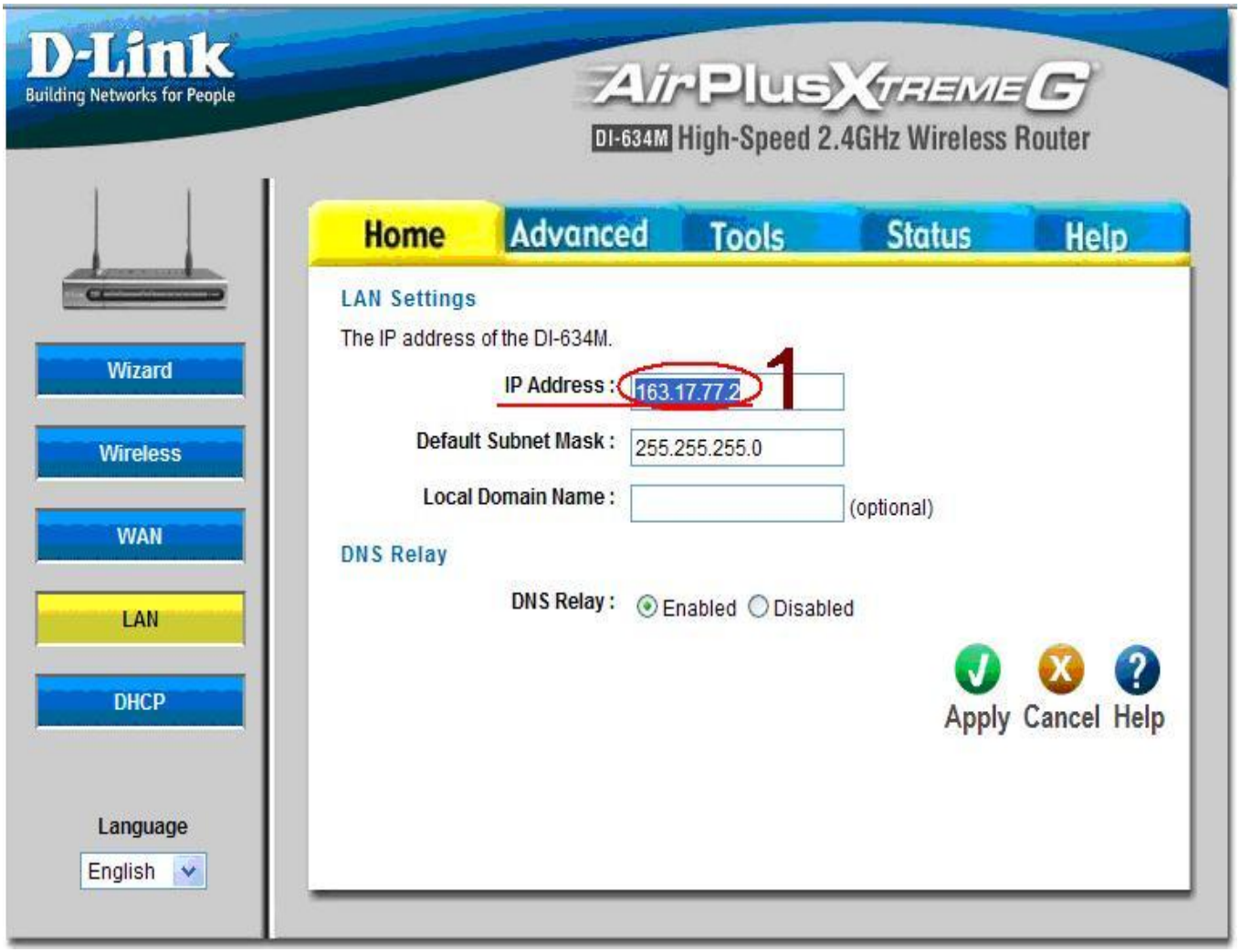


圖 3.3.11 Infrastructure(AP*2)架構 AP 位址設定頁面(IP Address)

3.在設定畫面點選左方的 Wireless 按鈕，進行 SSID 欄位的名稱輸入，如下

設定 D-Link 的 SSID 為 DLINK2(如~畫面中的數字標示 1)

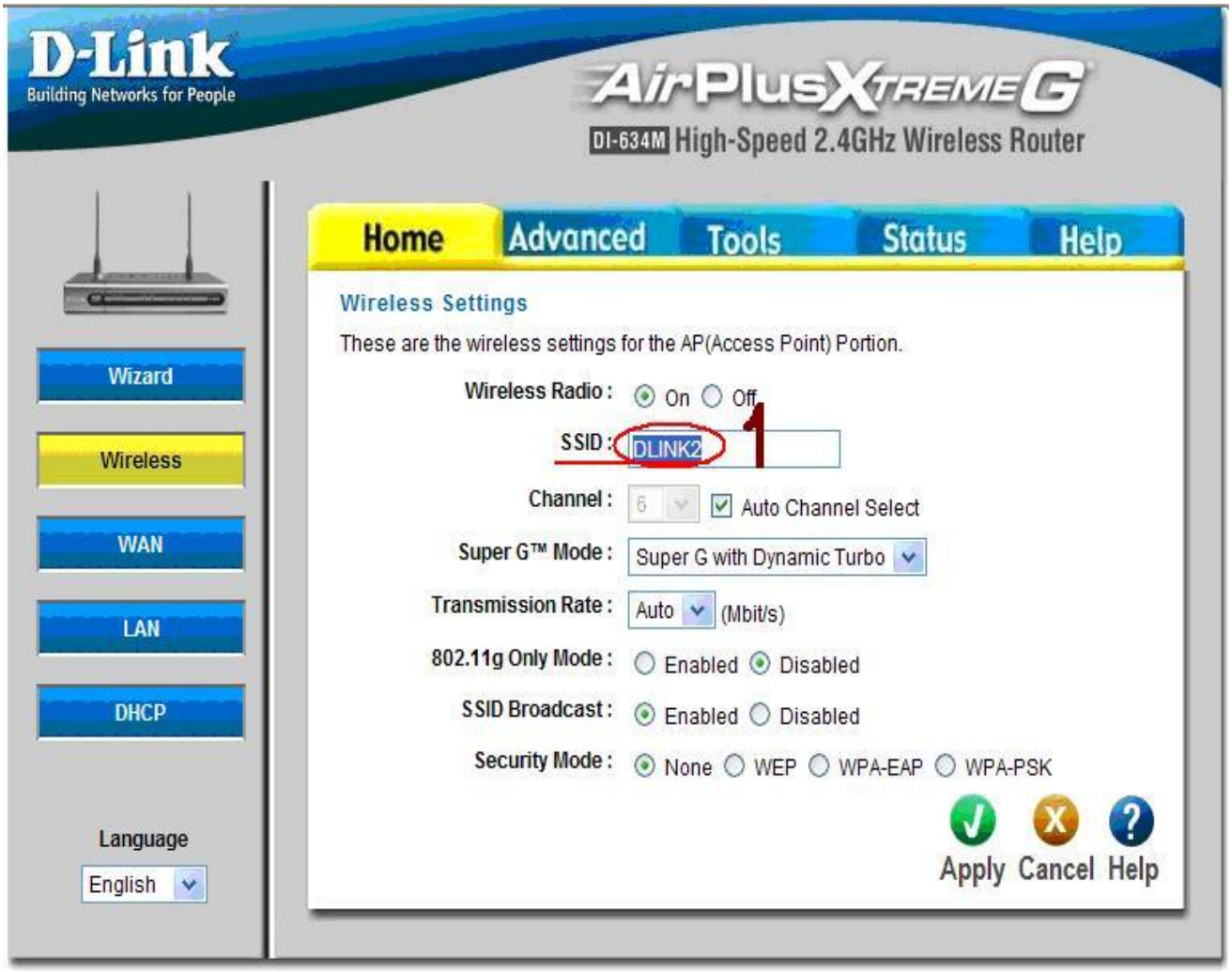


圖 3.3.12 Infrastructure(AP*2)架構 SSID 設定頁面

4.進入桌面工作列開始 →執行的視窗，輸入 cmd 指令開啟命令提示畫面，使用關鍵字 ipconfig 的指令顯示出先前 PC2 電腦設定的 IP 位址相關訊息(如~畫面中的數字標示 1)，並使用關鍵字 ping 的指令得到 PC2 經測試可順利連上 DLINK2(AP) (如~畫面中的數字標示 2)。

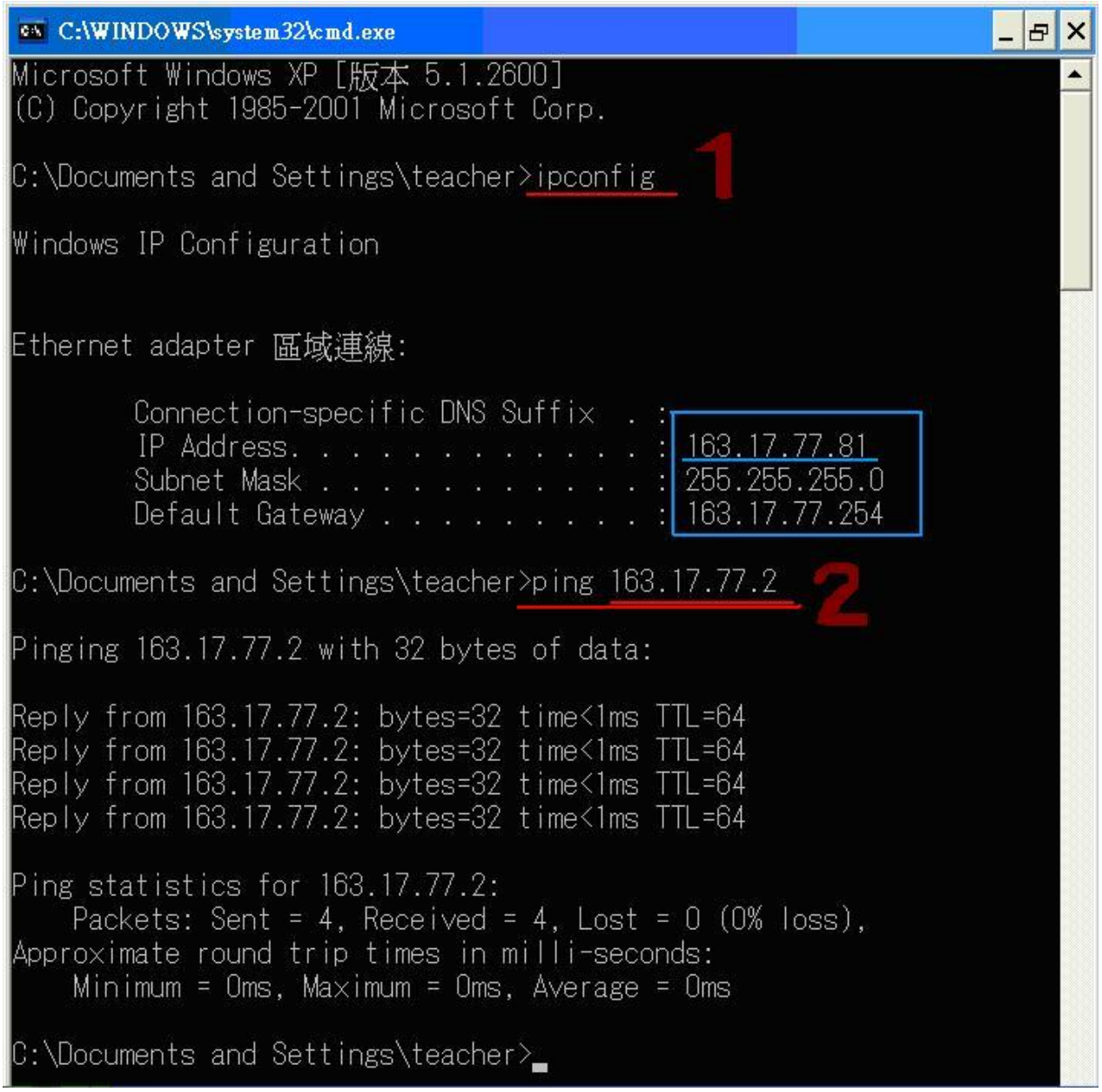


圖 3.3.13 Infrastructure(AP*2)架構 命令提示視窗操作- PC2 電腦

5.進入 NB2 筆記型電腦的無線網路連線內容，點選「TCP/IP 內容」開啟，設定與 D-Link2(AP)網站中相同網段的 IP 位址進行測試，如下

NB2 的 IP 設定

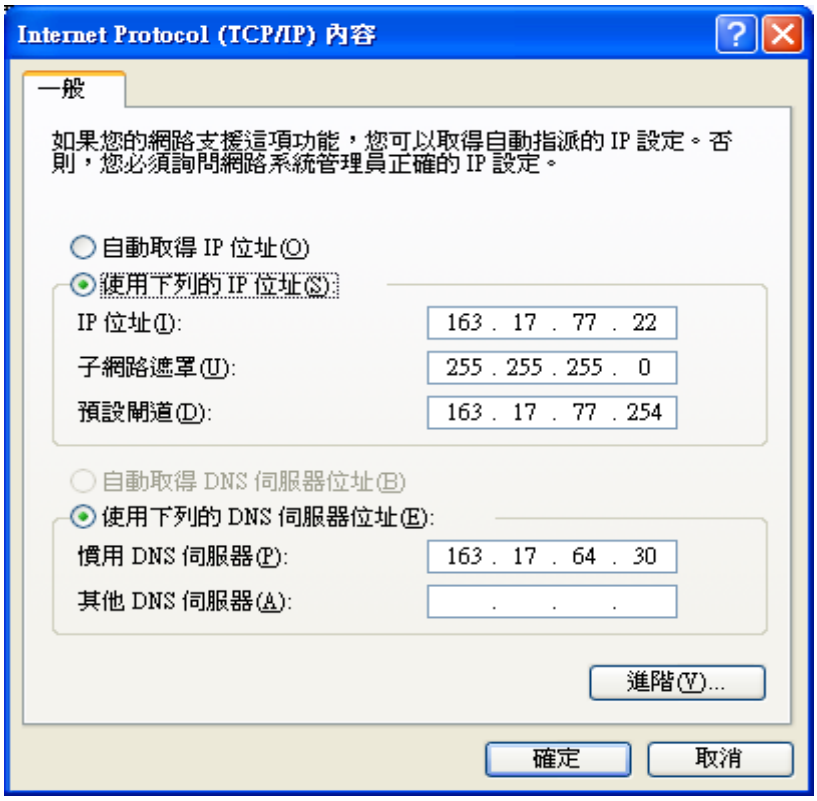


圖 3.3.14 Infrastructure(AP*2)架構 設定 NB2 筆記型電腦 IP 位址

6.進入網路連線的視窗，在無線網路連線的圖示上按右鍵點選「檢視可用的無線網路」開啟視窗畫面，如下圖。 在視窗左方點選重新整理網路清單，會偵測到比較近的 DLINK2(SSID)，並自動連線。

圖 3.3.15 Infrastructure(AP*2)架構 「無線網路連線」視窗- NB2 筆記型電腦

7.進入桌面工作列開始→執行的視窗，輸入 cmd 指令開啟命令提示畫面，使用關鍵字 ipconfig 的指令顯示出在 NB2 筆記型電腦所設定的 IP 位址(如~畫面中的數字標示 1)，並使用關鍵字 ping 的指令檢查是否與 PC2 電腦、DLINK2(AP)接通了，如下

指令：ping 163.17.77.2 →網站上設定 DLINK2(AP)的 IP 位址(如~數字標示 2)

ping 192.168.0.81 →另一台 PC2 電腦的 IP 位址(如~數字標示 3)

由關鍵字 ping 的測試，NB2 可透過 DLINK2 連接到 PC2 電腦。

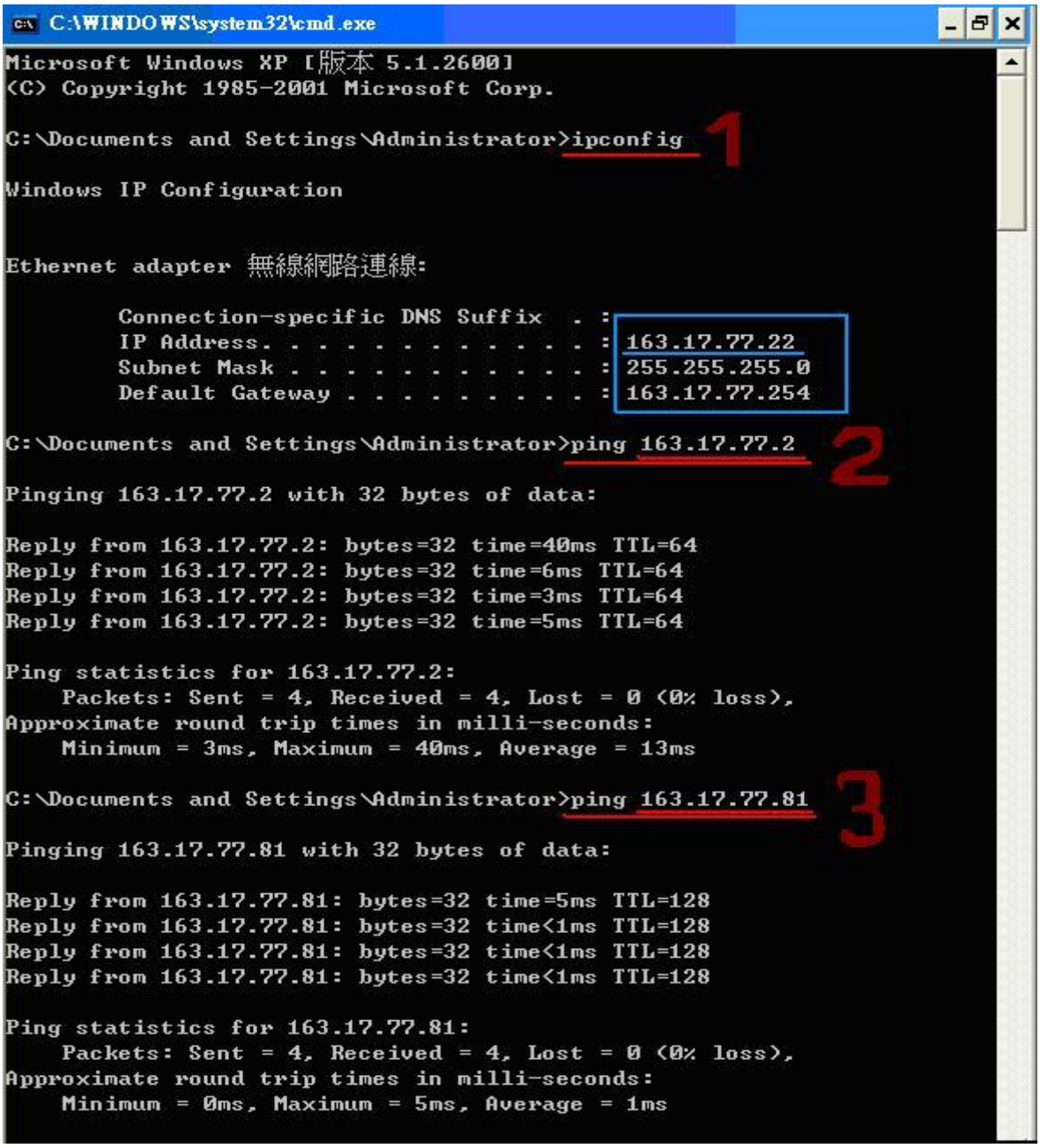


圖 3.3.16 Infrastructure(AP*2)架構 命令提示視操作- NB2 筆記型電腦

3.3.3 透過兩台 D-Link AP 的連接設定

(都順利連上後，透過兩台 AP(SSID=DLINK1 和 DLINK2)互相連接)

1.運用 PC1 電腦秀出 IP 位址(如~畫面中的數字標示 1)，去 ping 每一台 DLINK(AP)的位址(如~畫面中的數字標示 2→DLINK1 的位址、 畫面中的數字標示 3→DLINK2 的位址)。

PC1 測試

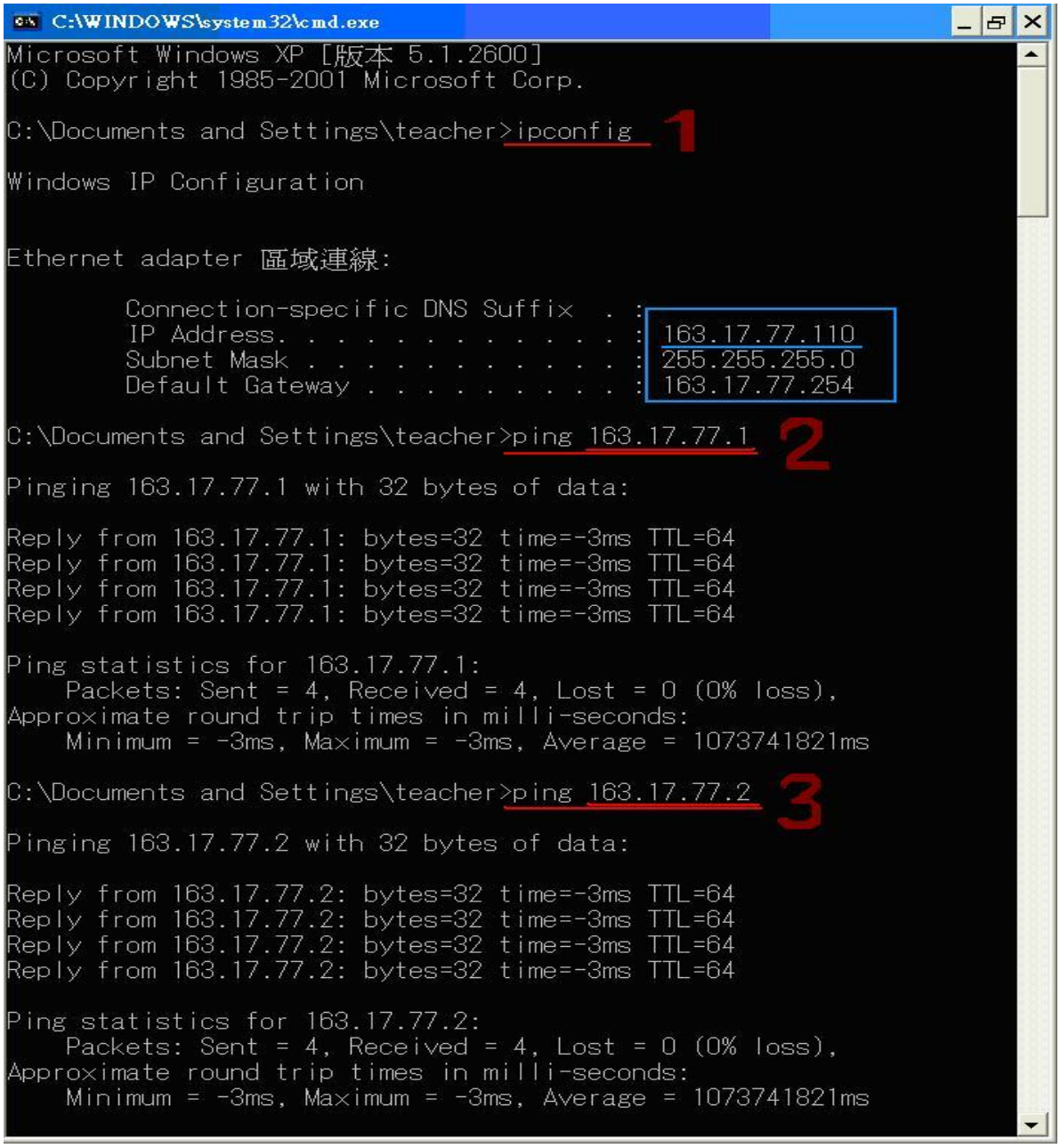


圖 3.3.17 Infrastructure(AP*2)架構 命令提示視窗-PC1 電腦測試 AP

2.運用 PC1 電腦，同樣去 ping 每一台電腦的 IP 位址，看看有沒有達到連線的功能。其中 NB1 筆記型電腦的 IP 位址是 163.17.77.11(如~畫面中的數字標示 1)，NB2 筆記型電腦的 IP 位址是 163.17.77.22(如~畫面中的數字標示 2)，PC2 電腦的 IP 位址是 163.17.77.81(如~畫面中的數字標示 3)。

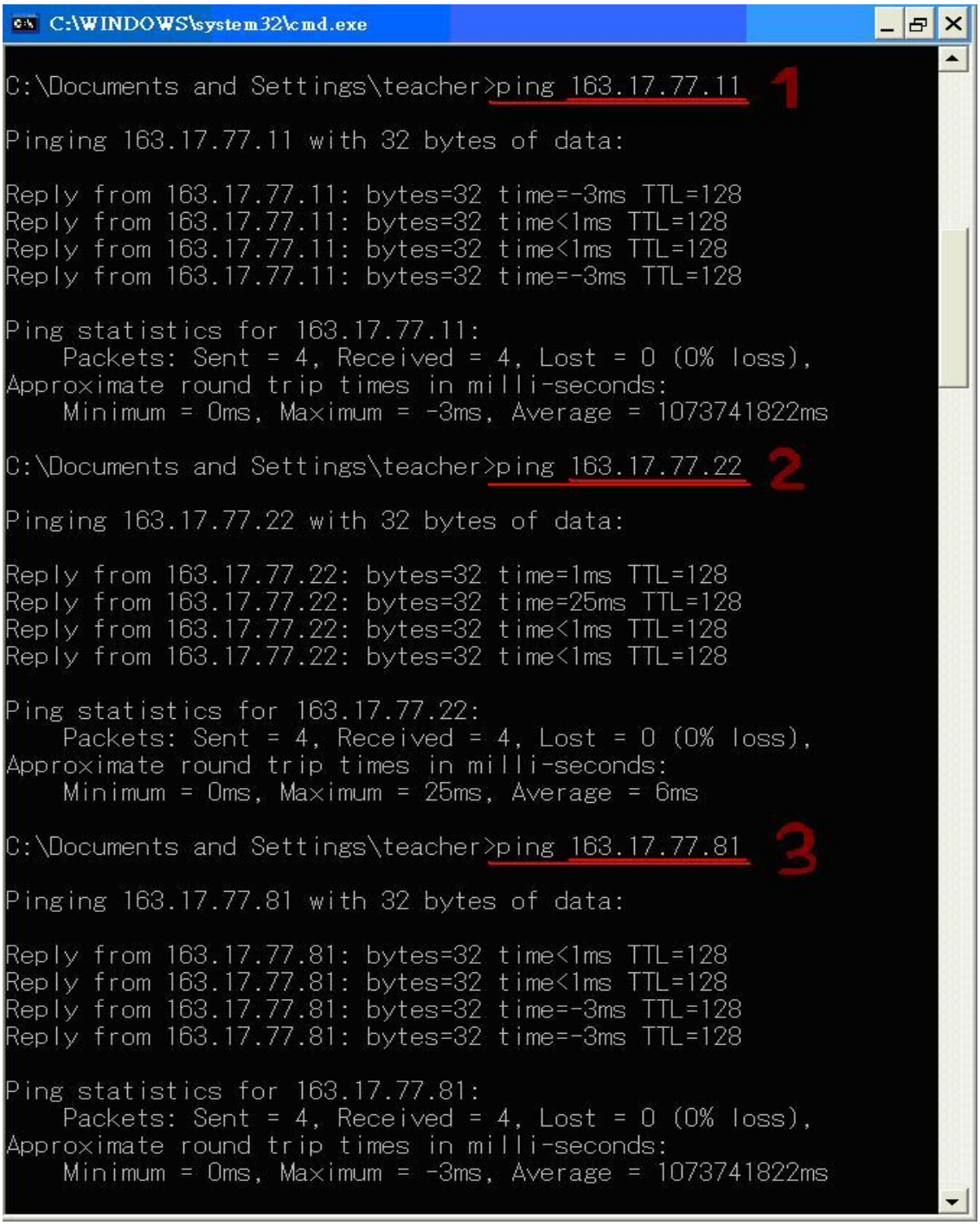


圖 3.3.18 Infrastructure(AP*2)架構 命令提示視窗-PC1 電腦

3.運用 PC1 電腦的 arp –a 指令，透過 DLINK1(數字標示 1)連上 DLINK2(數字標示 2)可和 NB1 筆記型電腦(數字標示 3)，NB2 筆記型電腦(數字標示 4)，PC2 電腦(數字標示 5)進行溝通。

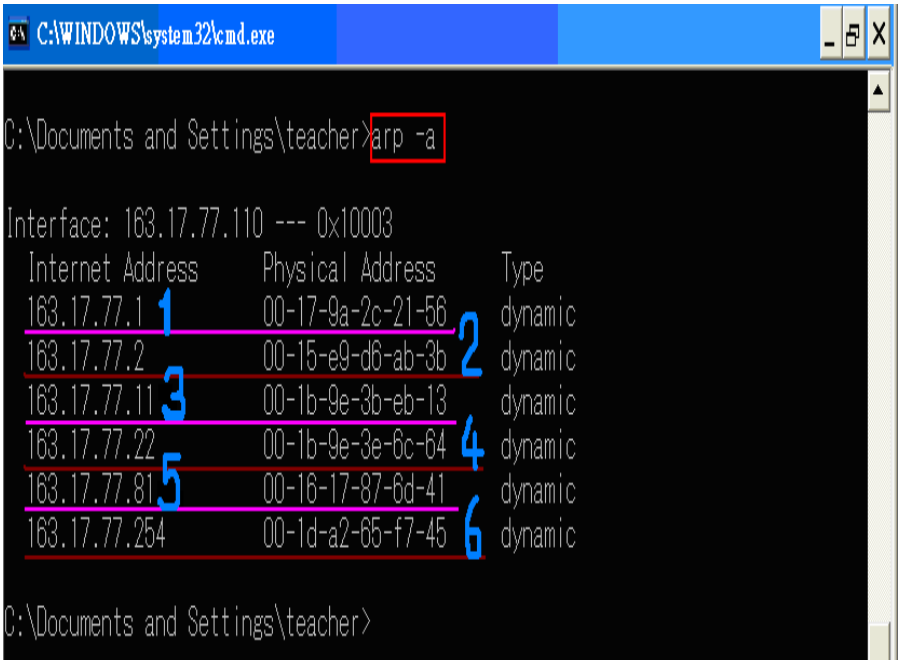


圖 3.3.19 Infrastructure(AP*2)架構 命令提示視窗-PC1 電腦秀出互連裝置

4.透過網路芳鄰找尋電腦去抓取對方檔案，輸入您想找的 IP 電腦位址(例如 163.17.77.11 便可找尋 NB1 的檔案)。

圖 3.3.20 Infrastructure(AP*2)架構 搜尋結果-PC1 電腦(a)

5.與上面同步驟打開網路上的芳鄰找尋電腦去抓取對方檔案，輸入您想找的 IP 電腦位址(例如 163.17.77.22 便可找尋 NB2 的檔案)。

圖 3.3.21 Infrastructure(AP*2)架構 搜尋結果-PC1 電腦(b)

6.與上面同步驟打開網路上的芳鄰找尋電腦去抓取對方檔案，輸入您想找的 IP 電腦位址(例如 163.17.77.81 便可找尋 PC2 的檔案)。

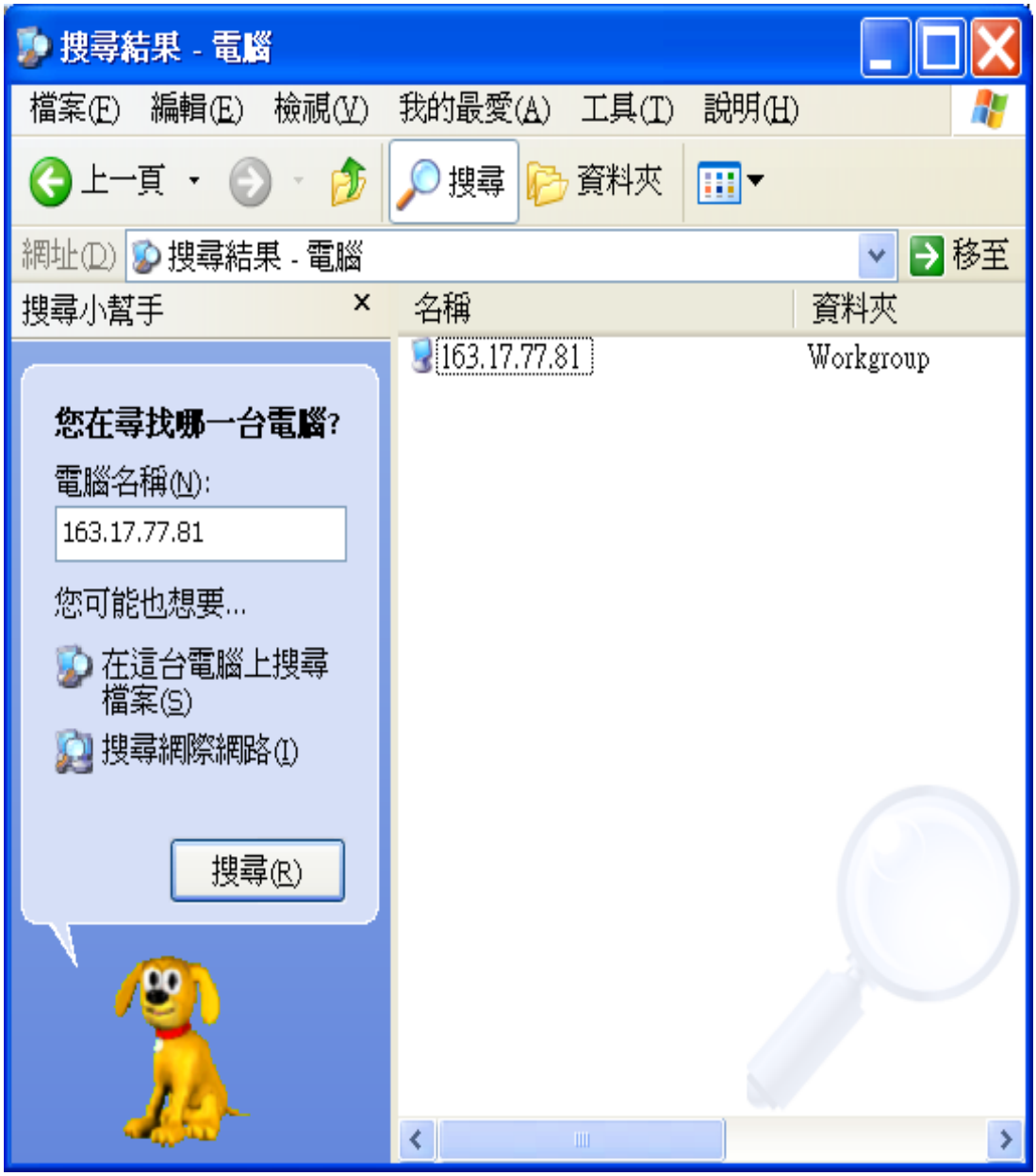


圖 3.3.22 Infrastructure(AP*2)架構 搜尋結果-PC1 電腦(c)

7.運用 ipconfig /all 指令秀出 PC1 網卡位址(如~畫面中的數字標示 1)，開啟 WireShark，點選上面的 Capture，再選取 AirPcap Interfaces 作封包過濾的設定。出現圖示右下的視窗後，點選 capture filter:，以設定 PC1 網卡位址的條件擷取封包(如~畫面中數字標示 2)。

進行擷取封包(ipconfig /all　秀網卡位址)

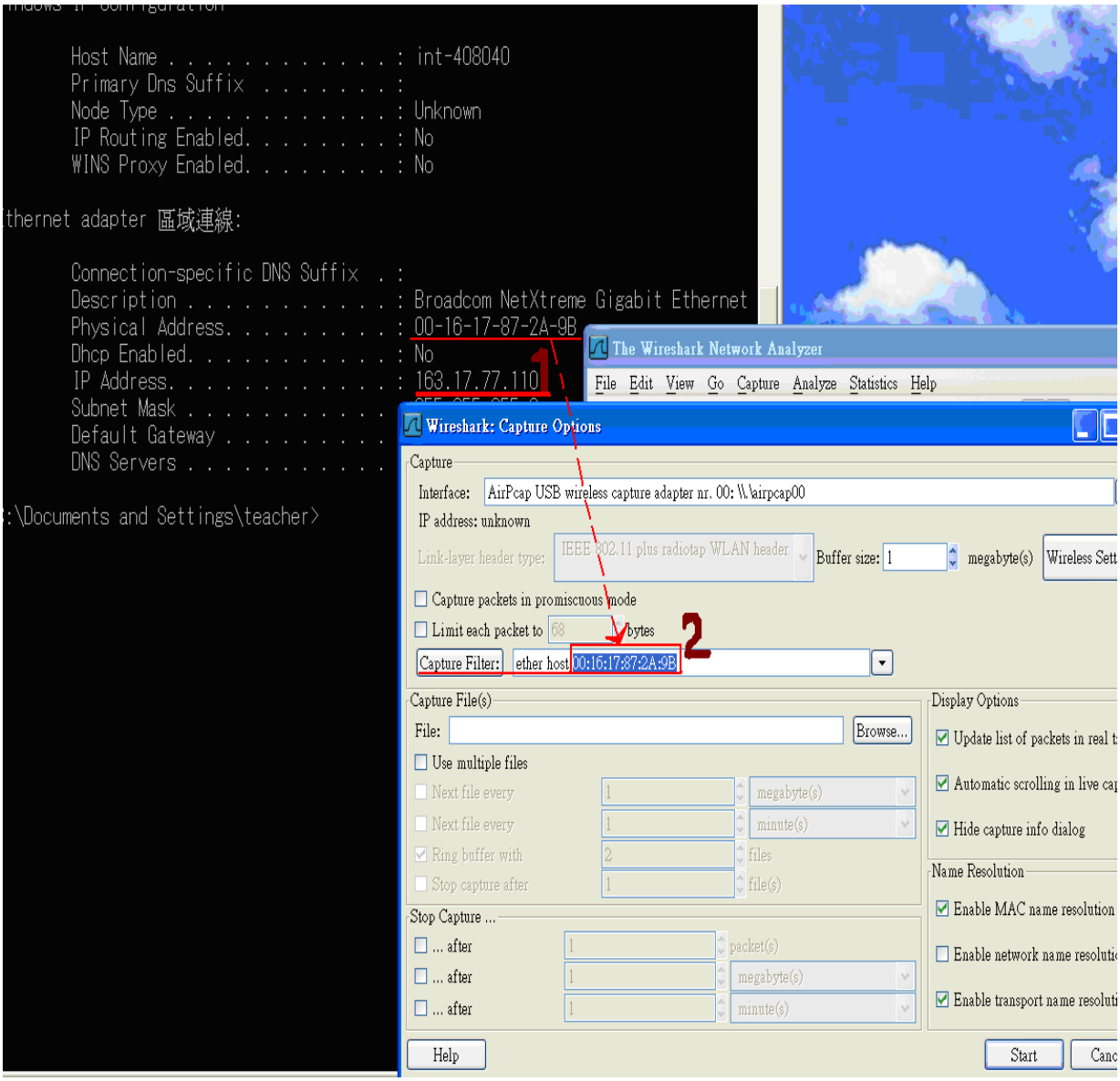


圖 3.3.23 Infrastructure(AP*2)架構 封包擷取前的過濾-PC1 電腦

8.檢視到封包所擷取下來的內容標示 1 是來源 IP 的位址(NB2 筆記型電腦)，而標示 2 則是擷取到目的地封包內容的 IP 位址(PC1 電腦)。對照著前面命令提示畫面的視窗 arp –a 輸出結果，下面的標示 1a 則是顯示來源 IP 的網卡編號(163.17.77.22←→00：1b：9e：3e：6c：64)，而標示 2b 則是擷取的目的地封包 IP 的網卡編號(163.17.77.110←→00：16：17：87：2a：9b)。

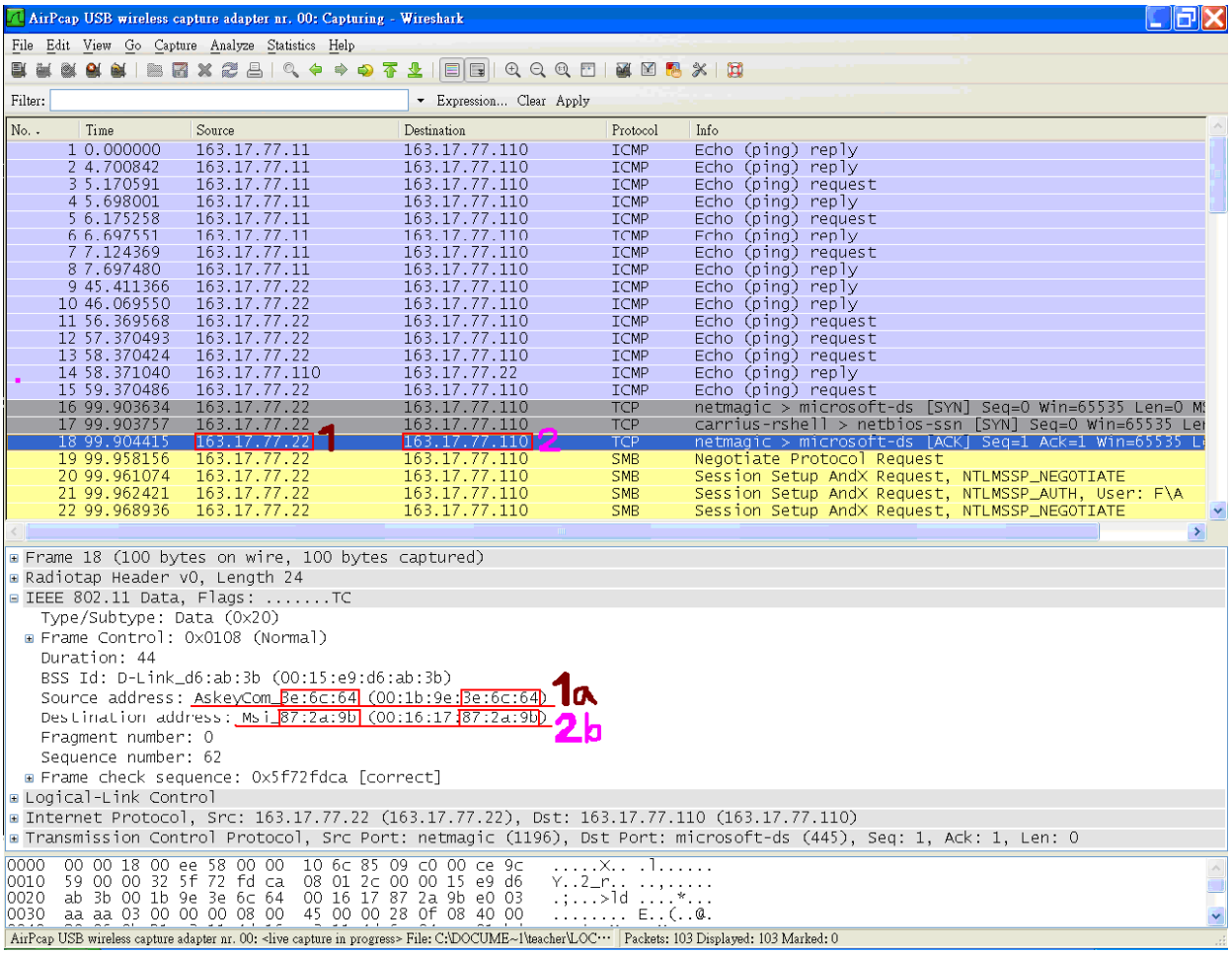


圖 3.3.24 Infrastructure(AP*2)架構 封包擷取結果- PC1 電腦

第四章 封包欄位解析

4.1 封包解析軟體 WireShark 介面與操作

如下面圖 4.1.1、圖 4.1.2 所示，進入 WireShark 封包擷取軟體，接上 USB 型式的外接式網卡 AirPacp，點選上方 Capture→開啟 Interfaces 視窗畫面，選擇 AirPcap 網卡介面的 Options 按鈕開始作封包過濾設定。

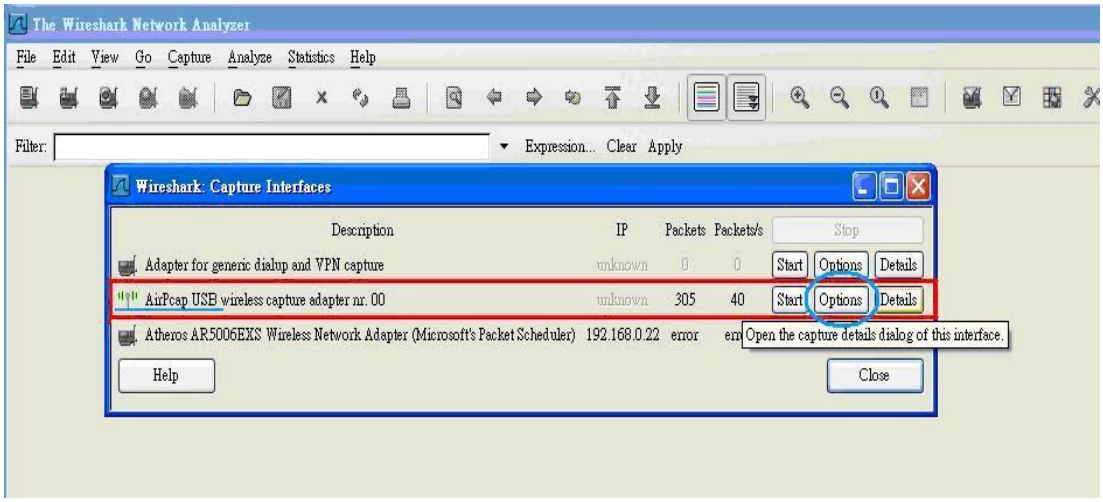


圖 4.1.1 封包擷取前的過濾設定(1)

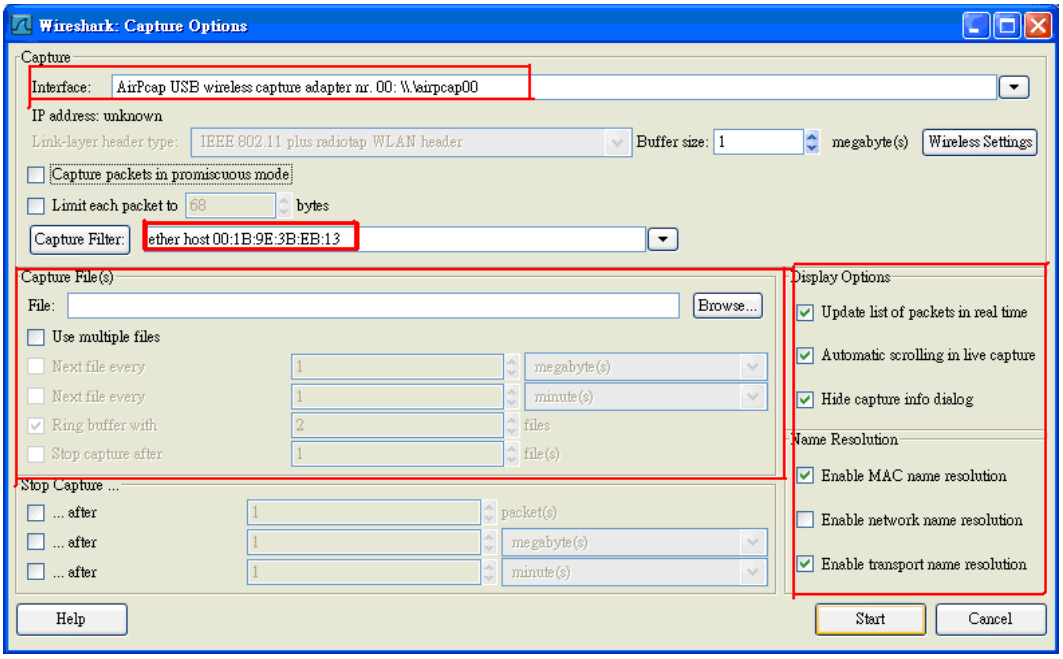


圖 4.1.2 封包擷取前的過濾設定(2)

使用 WireShark 時最常見的問題，是當你使用預設設置時，會得到大量冗余的封包訊息，所以很難找到自己需要的部份。這時就需要用過濾器下指令方便找尋我們要的封包。而過濾器又分為以下兩種

捕捉過濾器：用於決定將什麼樣的封包訊息紀錄在捕捉結果中，需要在開始捕捉前設置。

顯示過濾器：在捕捉結果中進行詳細找查，可以等到捕捉結果後隨意修改。

1.捕捉過濾器：(如圖 4.1.3、圖 4.1.4)

設置捕捉過濾器的步驟是：選擇 capture —>options 填寫〝capture filter〞欄或者點擊〝capture filter〞按鈕為你的過濾器取一個名字並保存，以便在日後捕捉繼續使用這個過濾器。點擊 Options 開始捕捉。

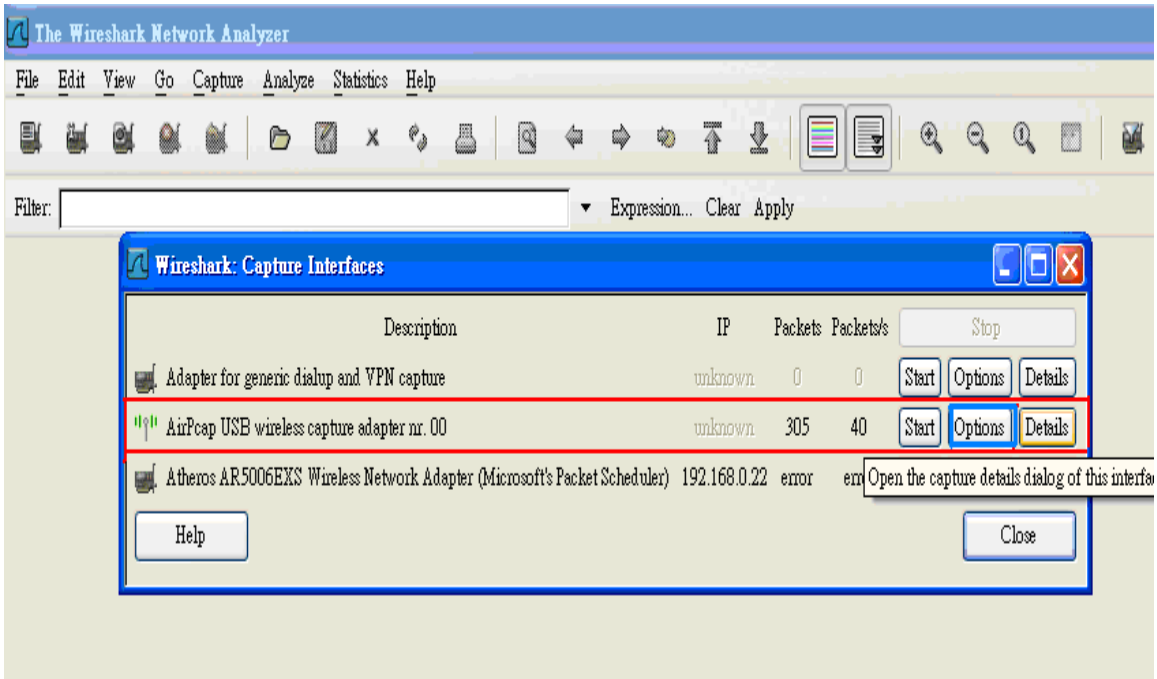


圖 4.1.3 封包過濾種類-捕捉過濾器(a)

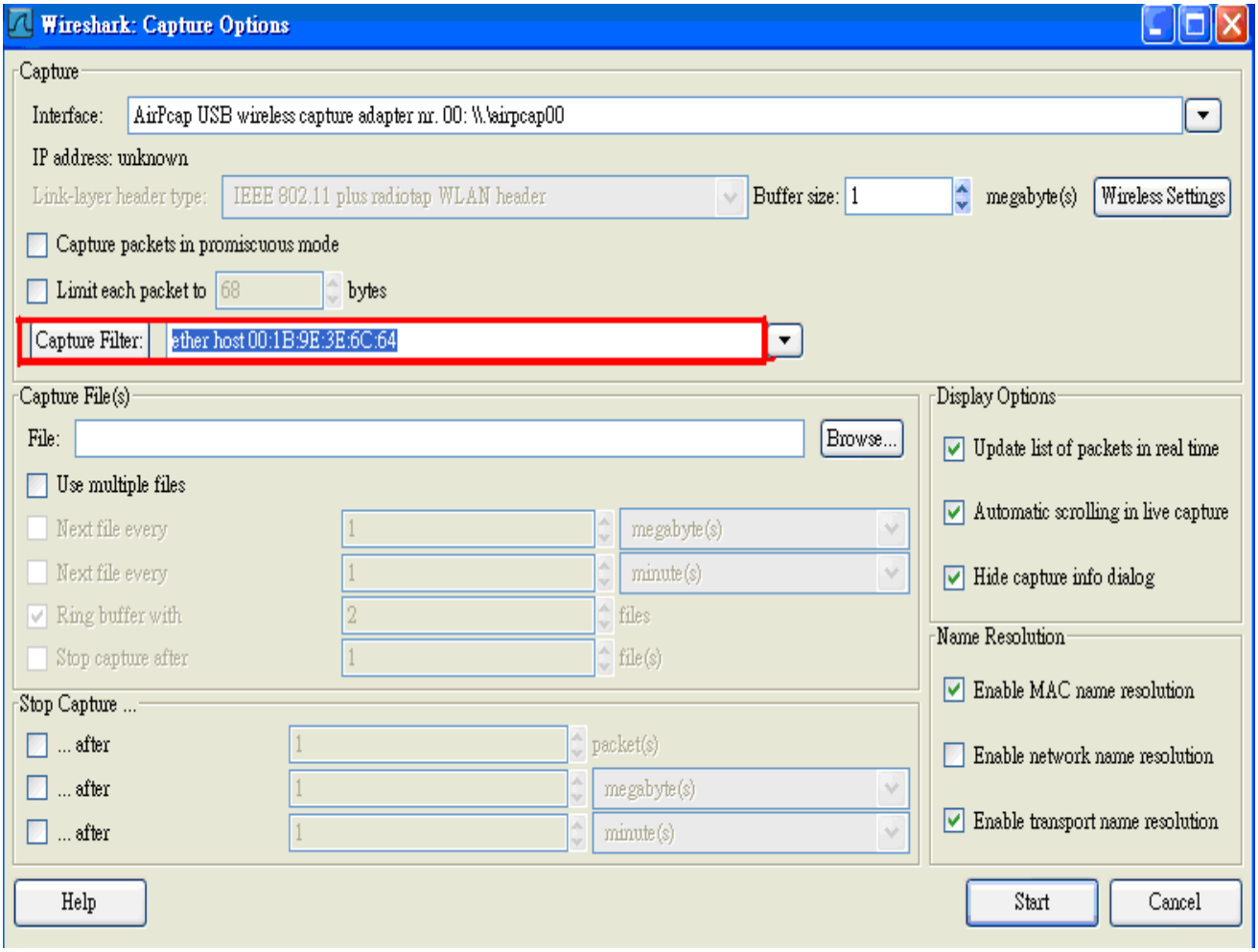


圖 4.1.4 封包過濾種類-捕捉過濾器(b)

語法：	Protocol	Direction	Host(s)	Value	Logical Operations	Other expression
例子：	tcp	dst	10.1.1.1	80	and	tcp dst 10.2.2.2 3128

Protocol（協議）

可能的值: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

如果沒有特別指明是什麼協議，則默認使用所有預設支持的協議。

Direction（方向）

可能的值: src, dst, src and dst, src or dst

如果沒有特別指明來源或目的地，則默認使用 "src or dst" 作為關鍵字。

例如，"host 10.2.2.2"與"src or dst host 10.2.2.2"是一樣的。

Host(s)
可能的值： net, port, host, portrange.
如果沒有指定此值，則默認使用"host"關鍵字。
例如，"src 10.1.1.1"與"src host 10.1.1.1"相同。

Logical Operations（邏輯運算）
可能的值：not, and, or.
否("not")具有最高的優先級。或("or")和與("and")具有相同的優先級，運算時從左至右進行。
例如，
"not tcp port 3128 and tcp port 23"與"(not tcp port 3128) and tcp port 23"相同。
"not tcp port 3128 and tcp port 23"與"not (tcp port 3128 and tcp port 23)"不同。

例子

```
tcp dst port 3128
```

顯示目的 TCP 埠為 3128 的封包。

```
ip src host 163.17.77.61
```

顯示來源 IP 地址為 163.17.77.61 的封包。

```
host 163.17.76.30
```

顯示目的或來源 IP 地址為 163.17.76.30 的封包。

2.顯示過濾器

通常經過捕捉過濾器過濾後的數據還是很複雜。此時可以使用顯示過濾器進行更加細緻的過濾。他的功能比捕捉過濾器更為強大，而且在你想修改過濾器條件時，並不需要重新捕捉一次。

語法：	Protocol	String 1	String 2	Comparison operator	Value	Logical Operations	Other expression
例子：	ftp	passive	ip	==	10.2.3.4	xor	icmp.type

Protocol（協議）:
您可以使用大量位於 OSI 模型第 2 至 7 層的協議。點擊"Expression..."按鈕後，您可以看到它們，如圖 4.1.5、圖 4.1.6 所示。
比如：IP，TCP，DNS，SSH

針對網路封包所使用的通訊協定，WireShark 在預設的情況下會啟用所有能夠辨識的通訊協定，不過使用者仍然可以自行選擇想要比對的通訊協定種類。

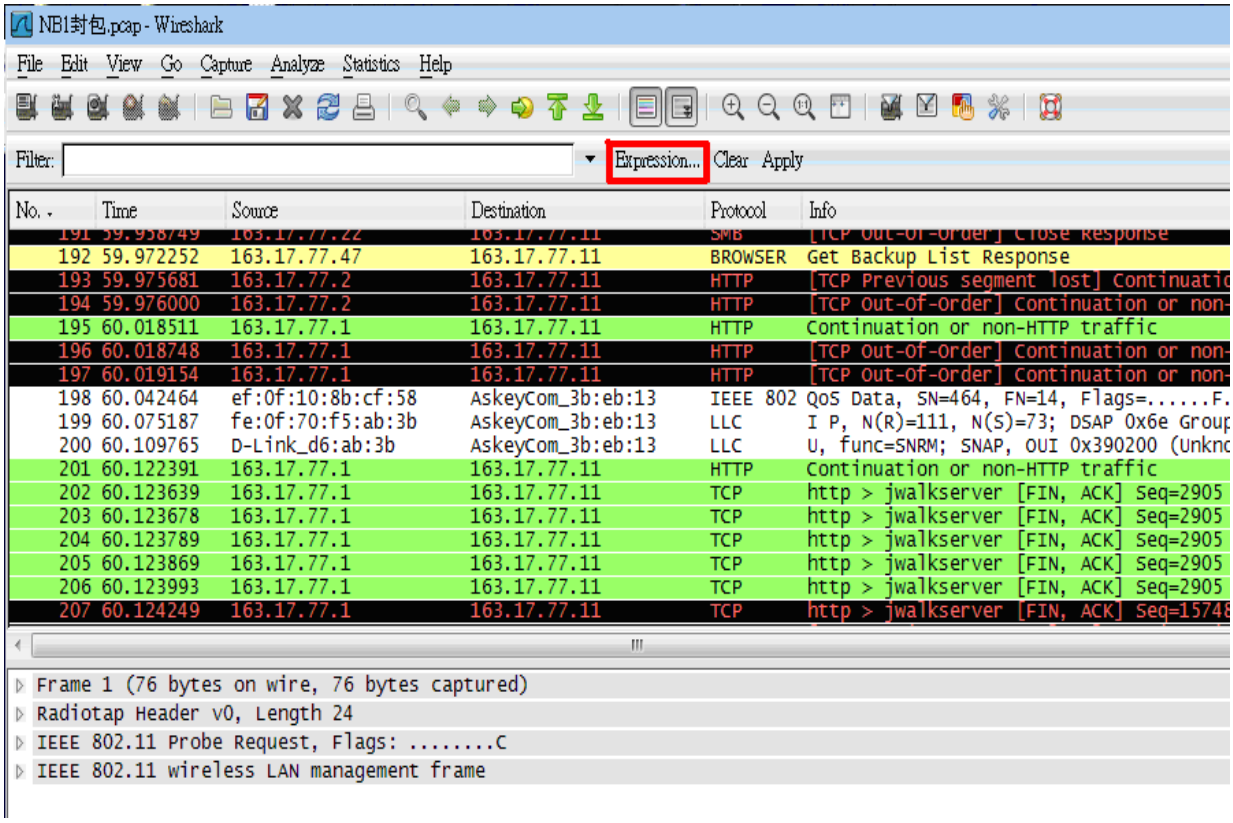


圖 4.1.5 封包軟體 WireShark 功能操作(Expression...鈕) -a

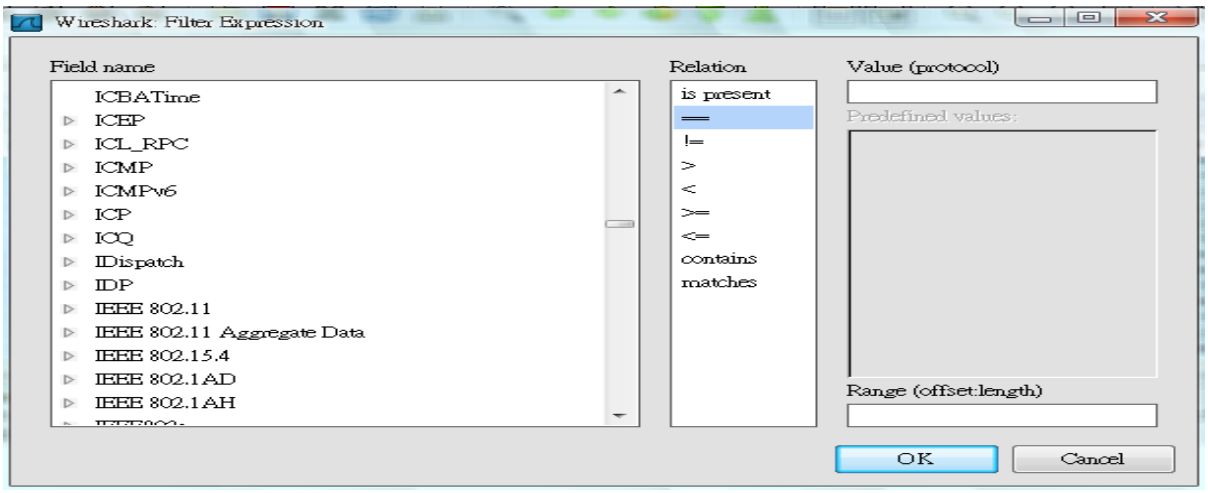


圖 4.1.6 封包軟體 WireShark 功能操作(Expression...鈕) -b

WireShark 完整的過濾器（Filter），使用者可以輸入關鍵字或條件，協助鎖定分析目標。在條件輸入的欄位內，如果使用的語法正確，底色將會變成綠色，反之，錯誤則會出現紅色底色。

ARP 是區域網路中常見的通訊協定，主要是用來查詢網路介面卡的實體位址。在區域網路中擷取封包時，若配合「arp」當作過濾的條件，將會發現如下圖 4.1.7 的畫面，在這裡可以發現許多廣播封包正詢問區域網路中是否存在這些電腦。

在正常情況下，如果在區域網路內收到這類型的網路封包已連上網路的主機將會進行回應，因為經常會看到一些閘道器（Gateway）或路由器（Router）發送出來的詢問封包，而這些封包正在找尋該網段中電腦或設備所使用的 MAC 位址。若配合過濾器，則必須輸入「arp」以作為過濾的條件，這樣可以很容易地將焦點聚集在 ARP 這個通訊協定上。

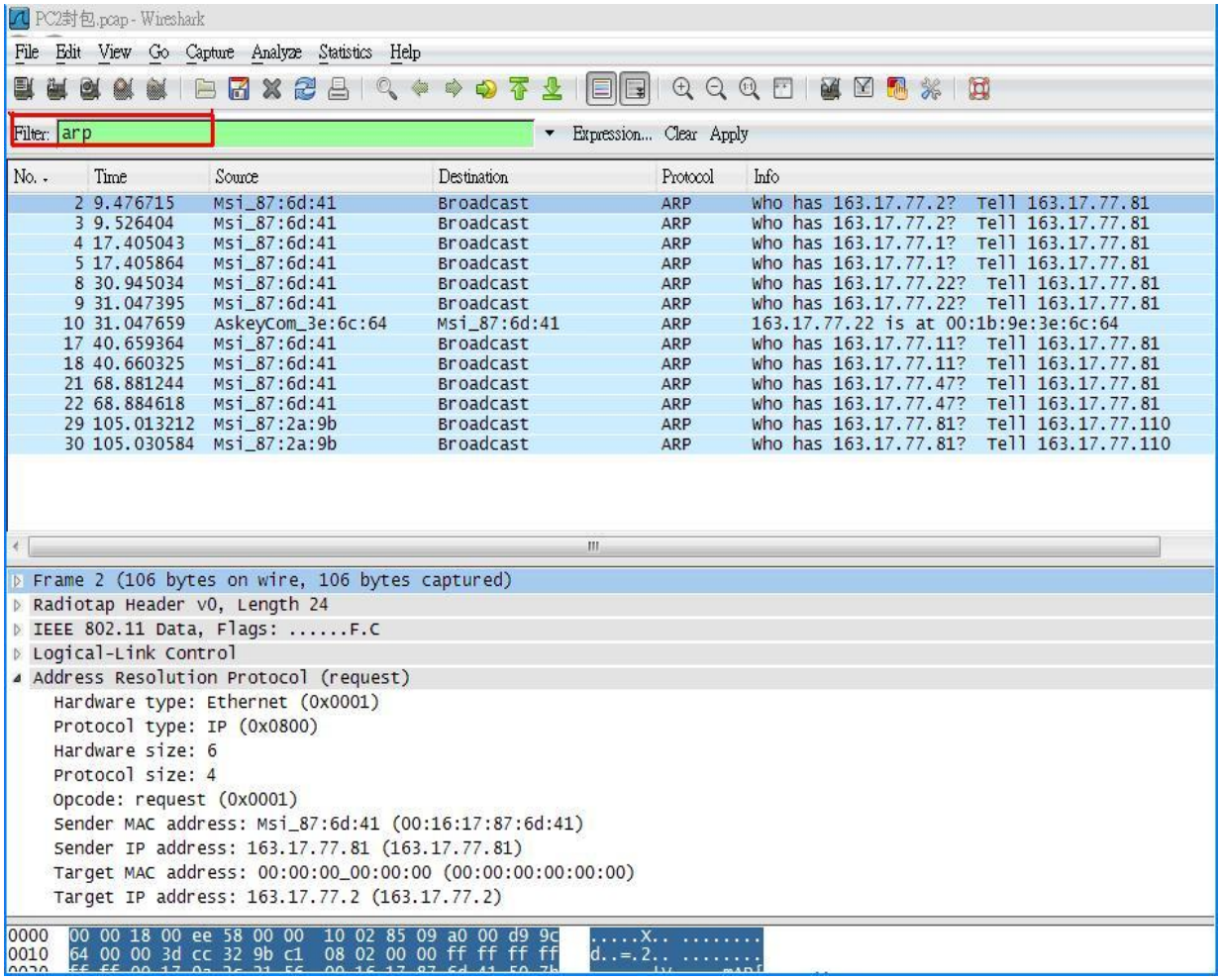


圖 4.1.7 封包軟體 封包資料過濾欄位

如下圖 4.1.8 所示，如果確定某些通訊協定並不存在於收集網路封包的環境中，則可以停用這些通訊協定，這在較繁忙的網路環境中將能降低比對的協定種類與數量，也可以避免因為硬體效能的問題而遺失原本打算擷取的網路封包。通訊協定清單中提供詳細的描述，可以做為是否啟用這些通訊協定的參考。

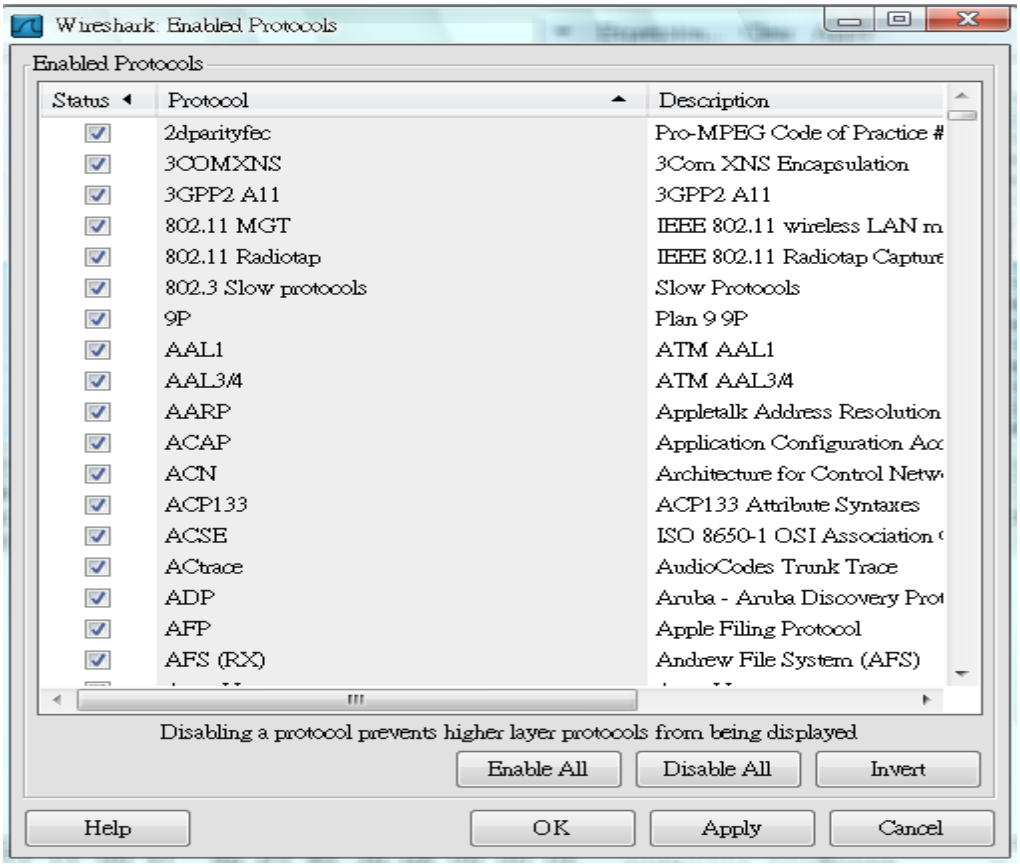


圖 4.1.8 封包軟體 通訊協定設定

你同樣可以在如下所示位置找到所支持的協議：(如圖 4.1.9、圖 4.1.10 所示)

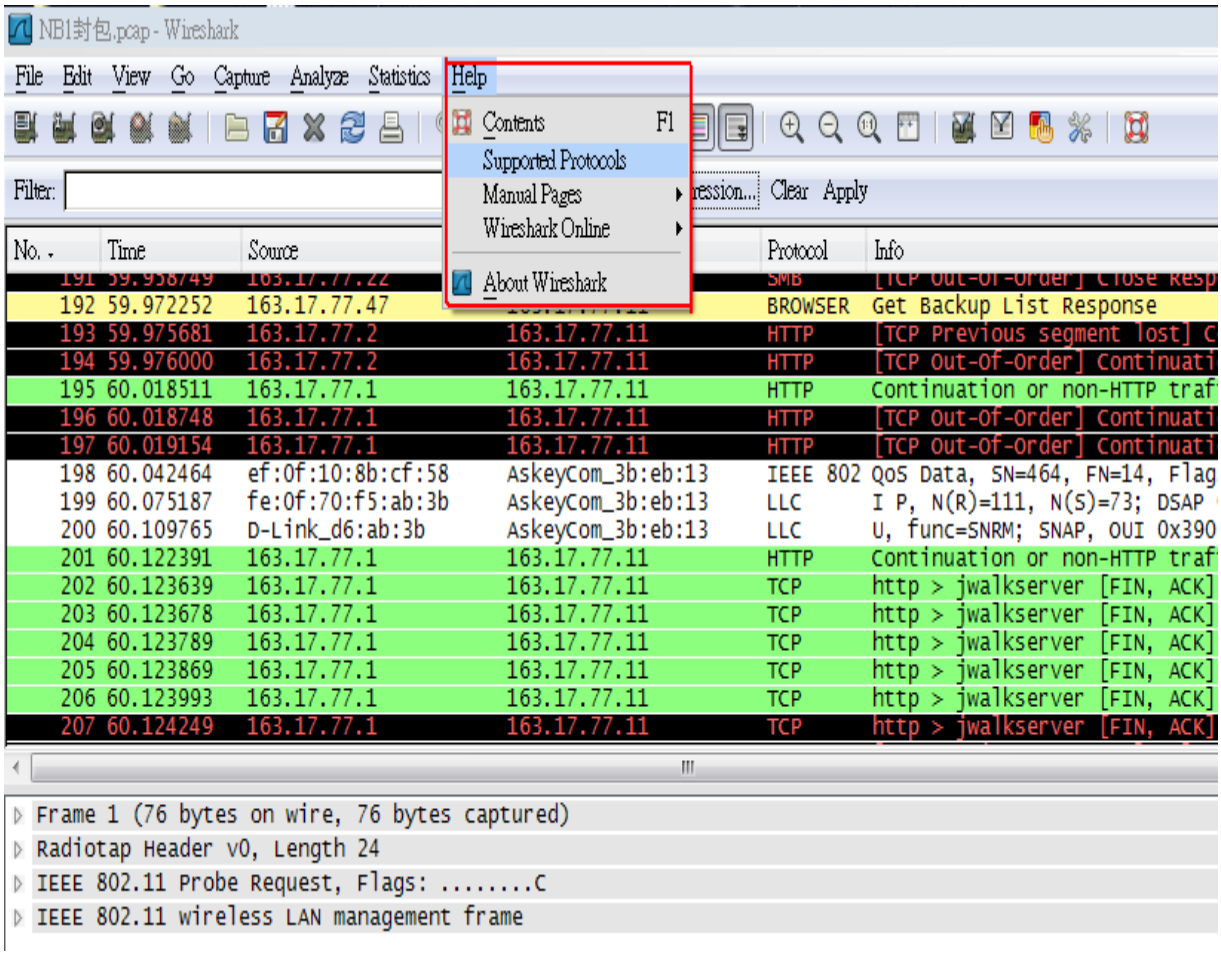


圖 4.1.9 封包軟體 相關協議查詢-a

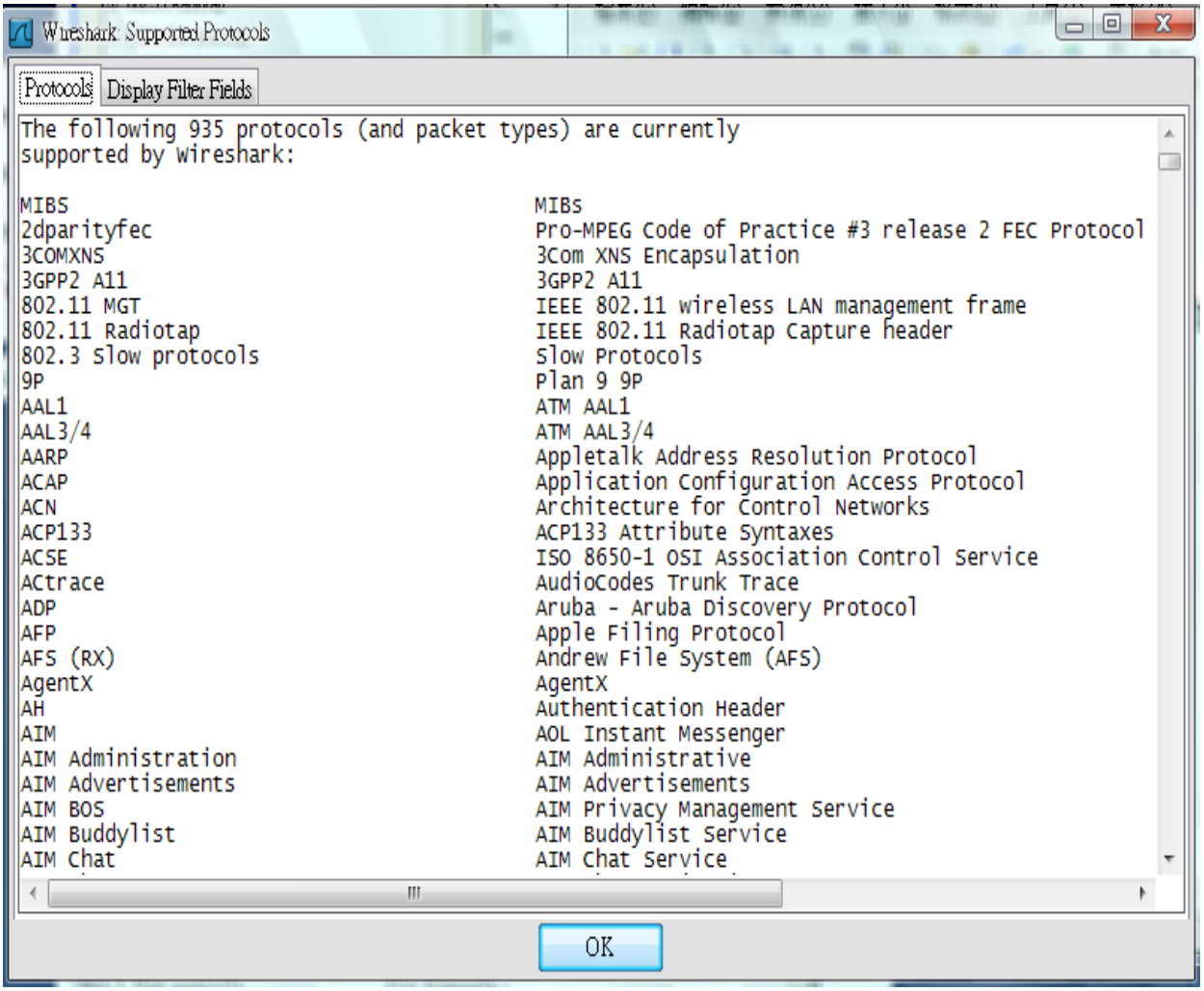


圖 4.1.10 封包軟體 相關協議查詢-b

Comparison operators （比較運算符）:

可以使用 6 種比較運算符

英文寫法	C 語言寫法	含義
eq	==	等於
ne	!=	不等餘
gt	>	大於
lt	<	小於
ge	>=	大於等餘
le	<=	小於等於

Logical expressions（邏輯運算符）

英文寫法	C 語言寫法	含義
and	&&	邏輯與
or	||	邏輯或
xor	^^	邏輯互斥或
not	!	邏輯非

例子

```
snmp || dns || icmp
```

顯示 SNMP 或 DNS 或 ICMP 封包

```
ip.addr==163.17.77.6
```

顯示來源或目的 IP 地址為 163.17.77.6 的封包

```
ip.src != 10.1.2.3 or ip.dst != 10.4.5.6
```

顯示來源不為 10.1.2.3 或者目的不為 10.4.5.6 的封包。
換句話說，顯示的封包將會為：
來源 IP：除了 10.1.2.3 以外任意；

目的 IP：任意以及來源 IP：任意；

目的 IP：除了 10.4.5.6 以外任意

```
tcp.port == 25
```

顯示來源或目的 TCP 埠號為 25 的封包。

善用右鍵

當發現有興趣進一步分析的網路封包，在點選該網路封包後，就可以透過滑鼠右鍵的快速功能表選單(如圖 4.1-11 所示)，直接指定交談時的過濾器，這樣就能夠很快地產生過濾條件或追蹤所指定網路封包或特定的通訊協定，並且自動填入過濾規則的欄位中。

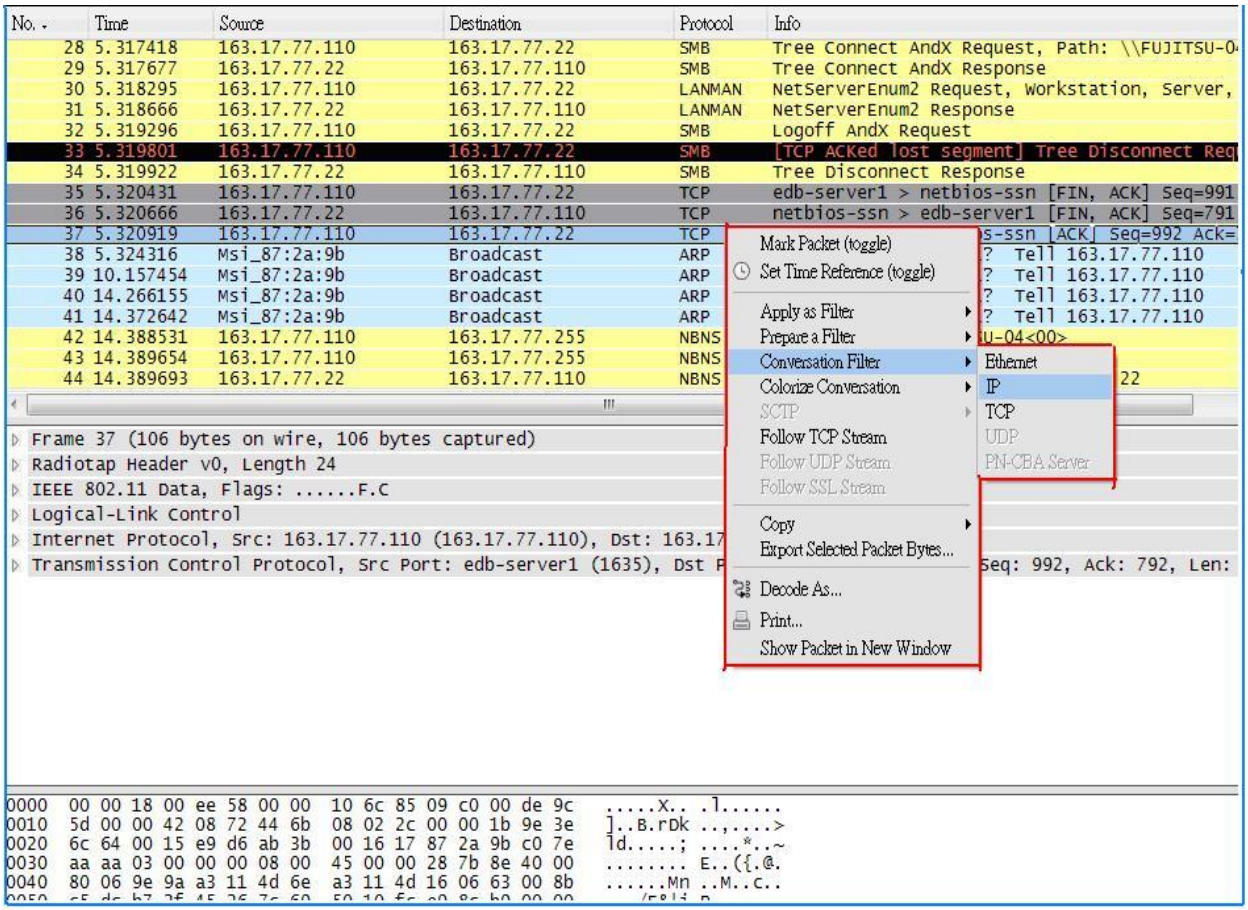


圖 4.1.11 封包軟體 右鍵封包過濾功能表

如下圖 4.1.12 所示，開啟之前在筆記型電腦(IP 位址：163.17.77.22)所截取到的封包檔案，會先看見來自多方面不同訊號的封包，此時可以在 Filter 欄位上(如~畫面中的數字標示 1)輸入相關指令過濾多餘封包資料，顯示出自己所要的封包。並且可以點選 Clear 按鍵(如~畫面中的數字標示 2)，取消封包的過濾，還原到原先多方面不同訊號的封包。

例如

1. 使用者可以先在 Filter 欄位以筆記型電腦的 IP 位址輸入指令

   →ip.addr == 163.17.77.22(先不用急著按下 Enter 鍵)。

2. 接著點選自行設定的 SSID 名稱(如~畫面中的數字標示 3)。

3. 在下方的封包資料中依序展開內容，尋找自行設定的 SSID 名稱 →“DLINK2”，並且在該欄位上按滑鼠右鍵，以 or 邏輯閘(||)的功能，進行封包的過濾(如~畫面中的數字標示 4)。

4. 此時將會秀出包含有 IP 位址和 SSID 名稱的所有封包。

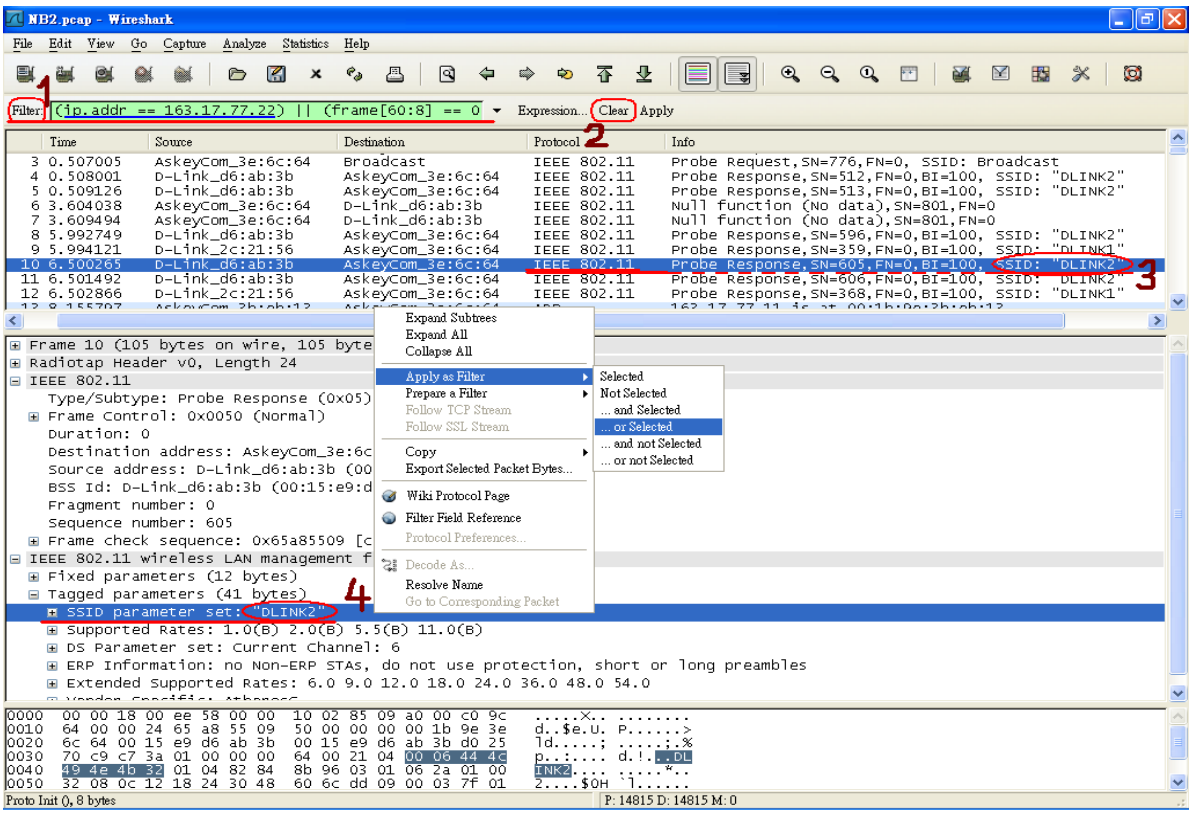


圖 4.1.12 封包軟體 封包過濾結果

接著來針對下方的封包資料作部份的介紹，如下：(如圖 4.1.13 所示)

1. Frame：代表第幾個封包，後面數字及單位代表封包的大小。例如畫面中代表第 77 個封包，為 211 Byte 大小的封包(如~畫面中的數字標示 1)。

2. Internet Protocol：代表 IP 位址，其中 Src 為來源端的 IP 位址、Dst 為目的地端的 IP 位址。例如畫面中 163.17.77.1 代表來源端的 IP 位址、而 163.17.77.22 代表目的地端的 IP 位址(如~畫面中的數字標示 2)。

3. Transmission Control Protocol：代表 TCP(縮寫)封包，而 Src Port 為連接埠號碼、Dst Port 為 Web Server 用的連接埠、Seq 為 Browser 隨機選取的起始續號、Ark 為 Browser 回應號碼、Len 為下一個傳回 Browser 的號碼(如~畫面中的數字標示 3)。

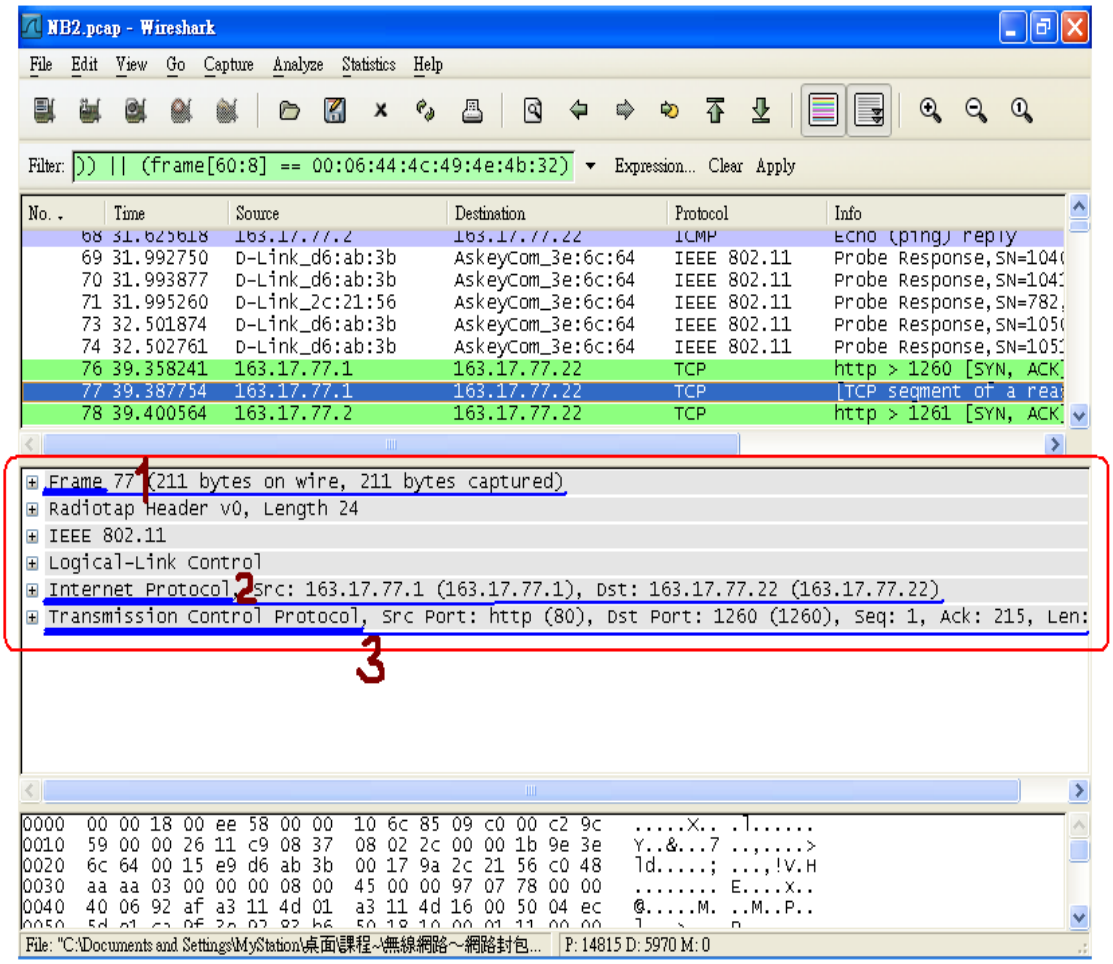


圖 4.1.13 封包軟體 封包資料欄位介紹

如下面圖 4.1.14 所示，要查看封包資料的相關內容，可點選上方有包含 IP 位址 163.17.77.22 的 ICMP 封包(如~畫面中的數字標示 1)，在下方展開 Internet Protocol 欄位的資料進行查看，其中 Version 代表 IP 規格的版本、Header length 代表標頭長度，而下面的數字資料，通常也都是以十六進位的方式列出來。

例如

1.從畫面上可看到 IP 規格的版本為 4，因此目前大部份的版本都為 4(如~畫面中的數字標示 2)。

2.而在下面的十六進位數字資料“45”，前面所表示的“4”是版本號數(第 1 點解釋)，而後面的“5”則表示標頭長度(如~畫面中的數字標示 3)。

3.在十六進位“5”的意思為，如果 Options 和 Padding 沒有設定的話，就只有 5 列的長度，因此長度為“5”；而每一列有 32 Bit 顯示出來，也就是 4 Byte；那麼 5 列就是 20 Byte(如~畫面中的數字標示 4)。

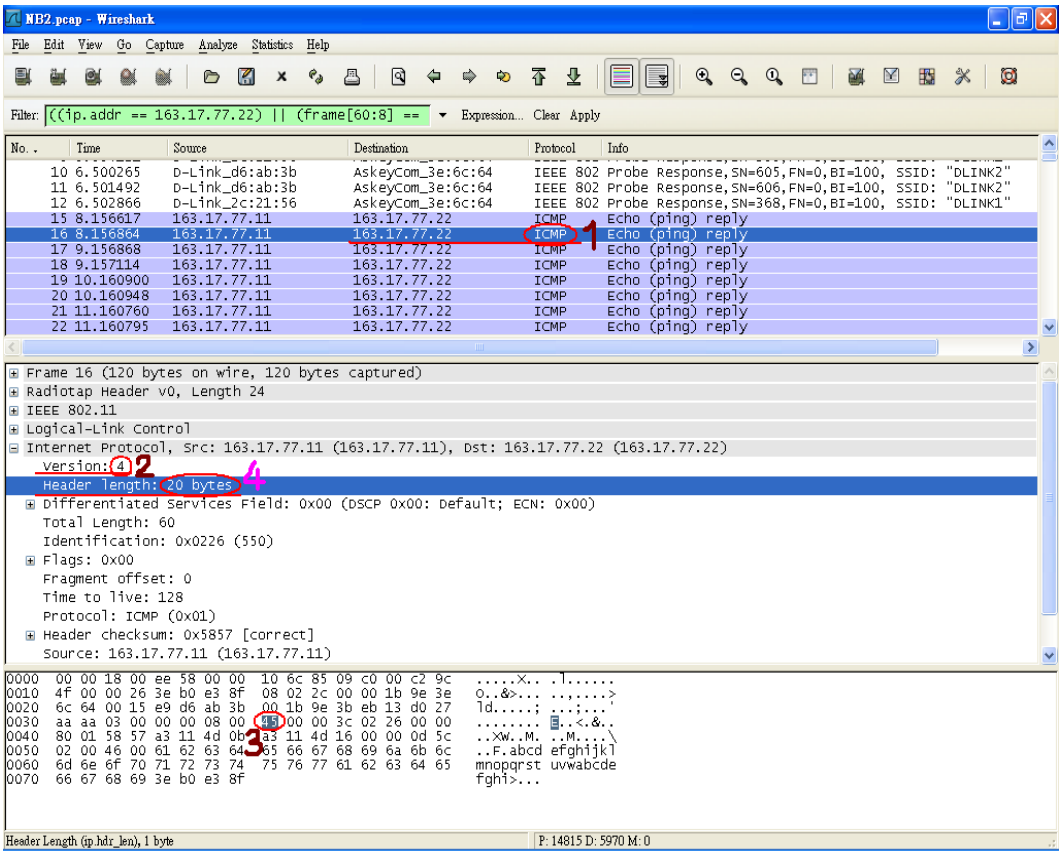


圖 4.1.14 封包軟體 IP 規格版本查詢(ICMP)

而 Time to live 所代表的是延續時間(TTL) (如下圖 4.15 所示)，在最下方的十六進位“80”經過換算後(如~畫面中的數字標示 1)，可得到十進位的 128，因此 TTL 為 128 個跳站(如~畫面中的數字標示 2)。

在 ICMP 協定當中的 TTL，是以封包路由過程中的跳站數目(Hop Count)做單位，每經過一個跳站(或被一個 router 處理)之後，TTL 值就會扣掉一個數值。 這樣就可以避免封包在傳送時，未能抵達目的地的時候一直停留在網路上面。

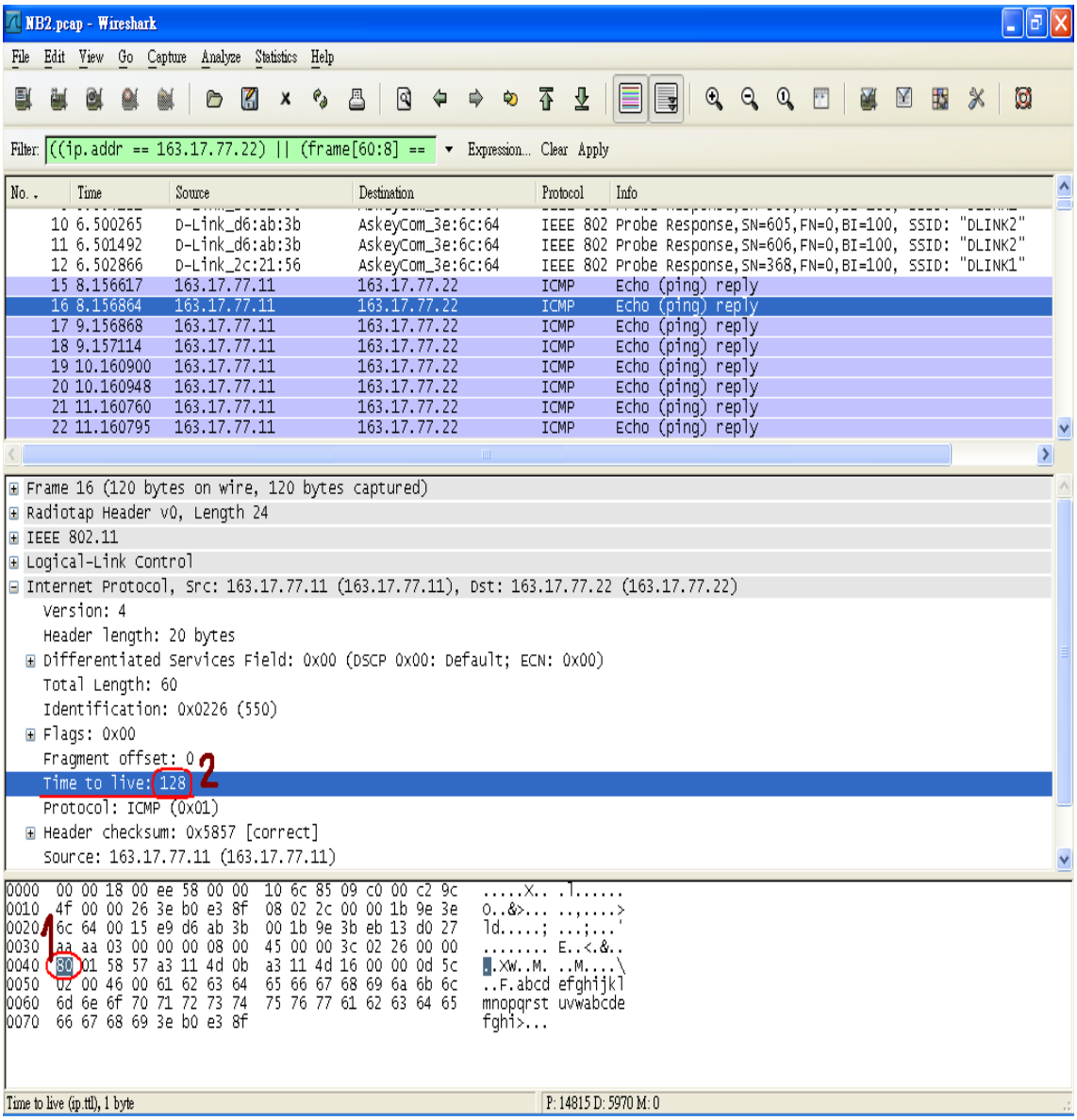
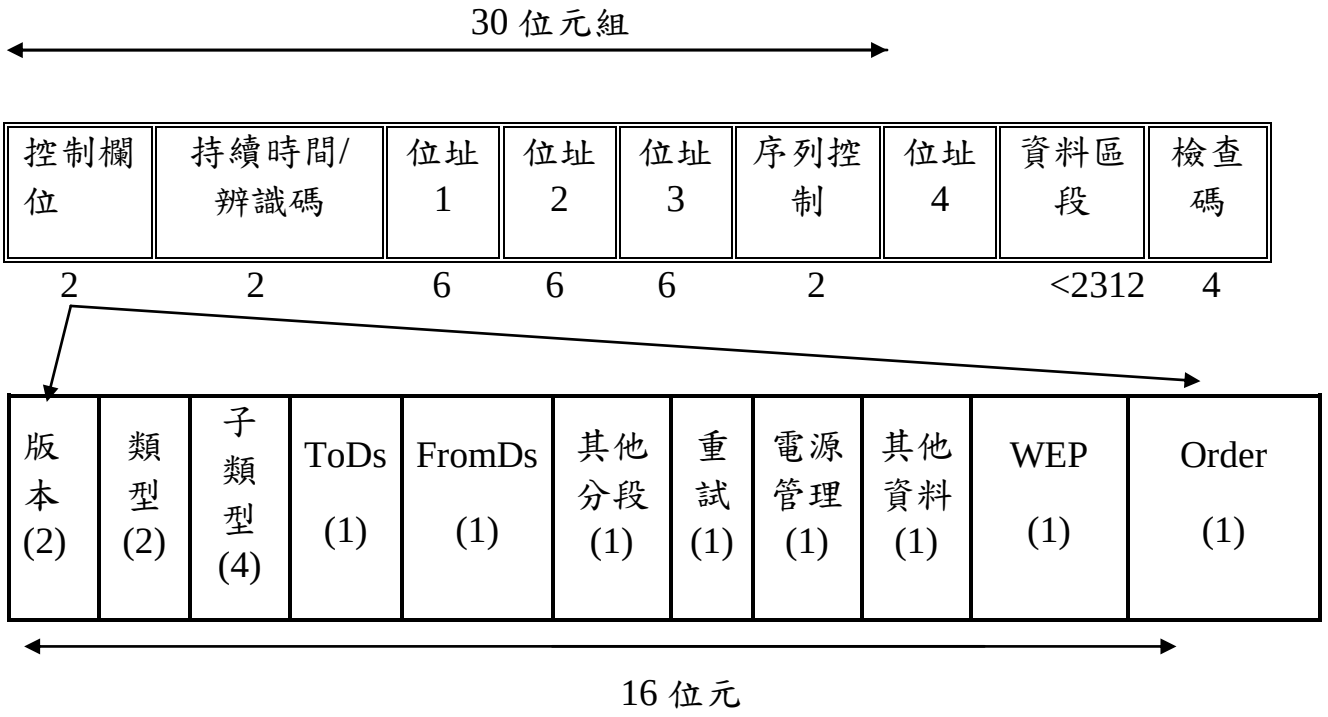


圖 4.1.15 封包軟體 延續時間(TTL)查詢

4.2 封包資料 IEEE 802.11 欄位解釋



IEEE 802.11 訊框格式(如圖 4.2.1 所示)

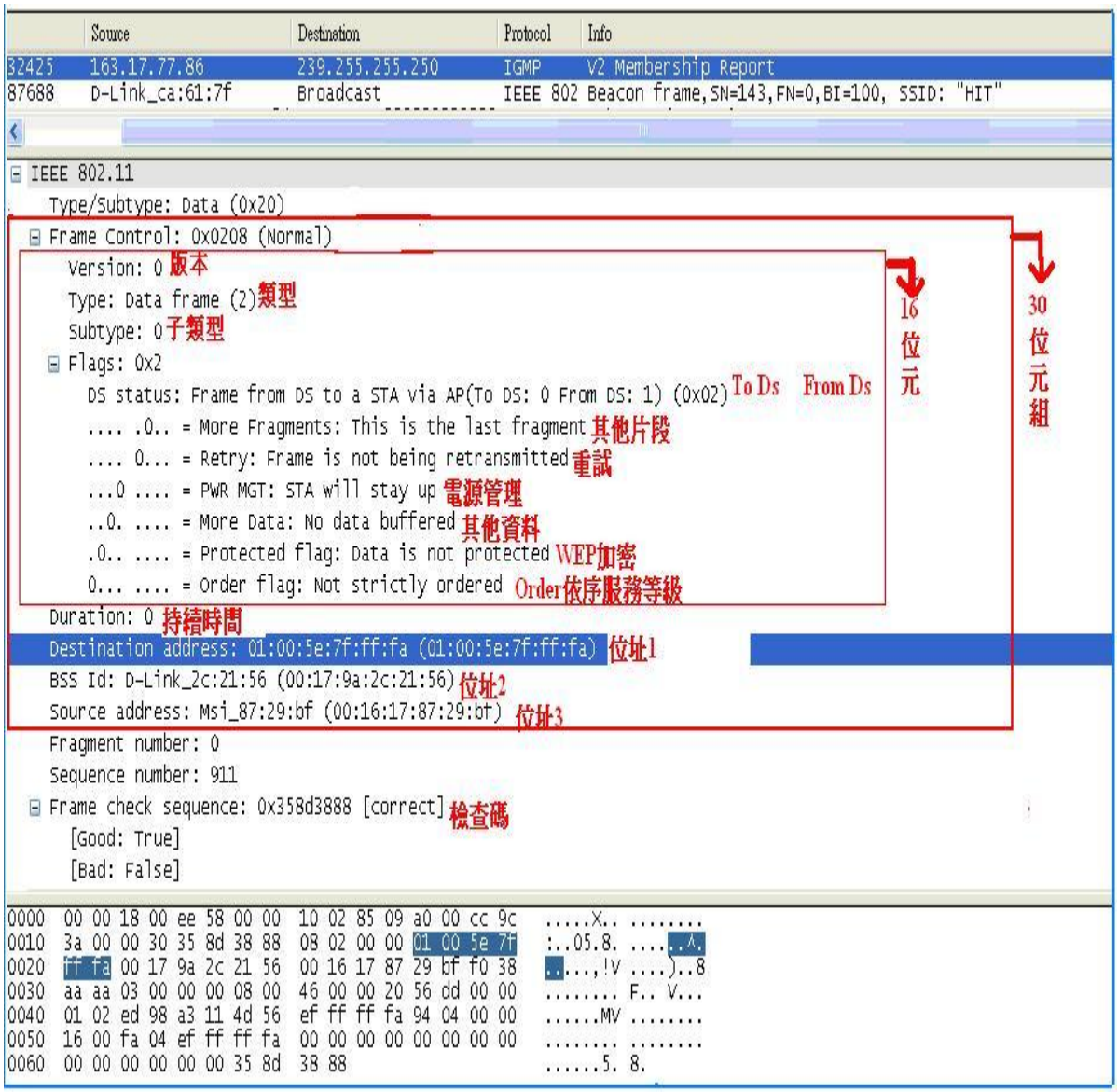


圖 4.2.1 封包資料 IEEE 802.11 欄位資料歸類

4.2.1 Frame Control 欄位- Version、Type、Subtype 介紹

版本(Version；2 位元)：(如下圖 4.2.2 所示)

說明 802.11 訊框的版本，目前這個欄位的值都設為 0。

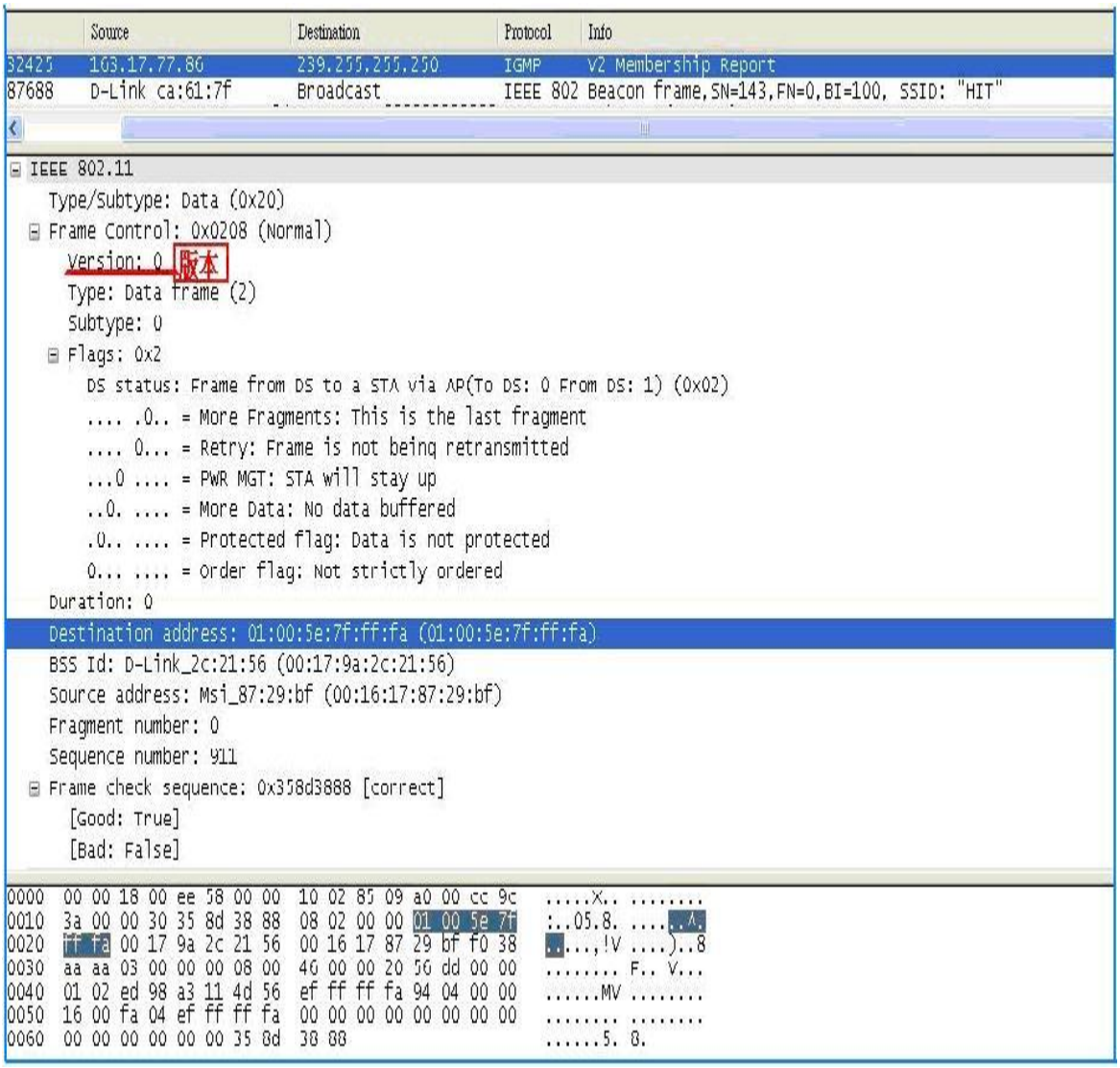


圖 4.2.2 封包資料 IEEE 802.11 欄位- 版本(Version)

類型(Type；2 位元)：(如下圖 4.2.3 所示)

802.11 訊框依屬性大致分為 3 類，分別是控制訊框(Control Frame)、資料訊框(Data Frame)與管理訊框(Management Frame)。三類訊框便以類型(Type)欄位來進行區分：00 代表管理類型、01 代表控制類型、10 代表資料屬性的訊框，而 11 則保留未使用，目前尚未定義。

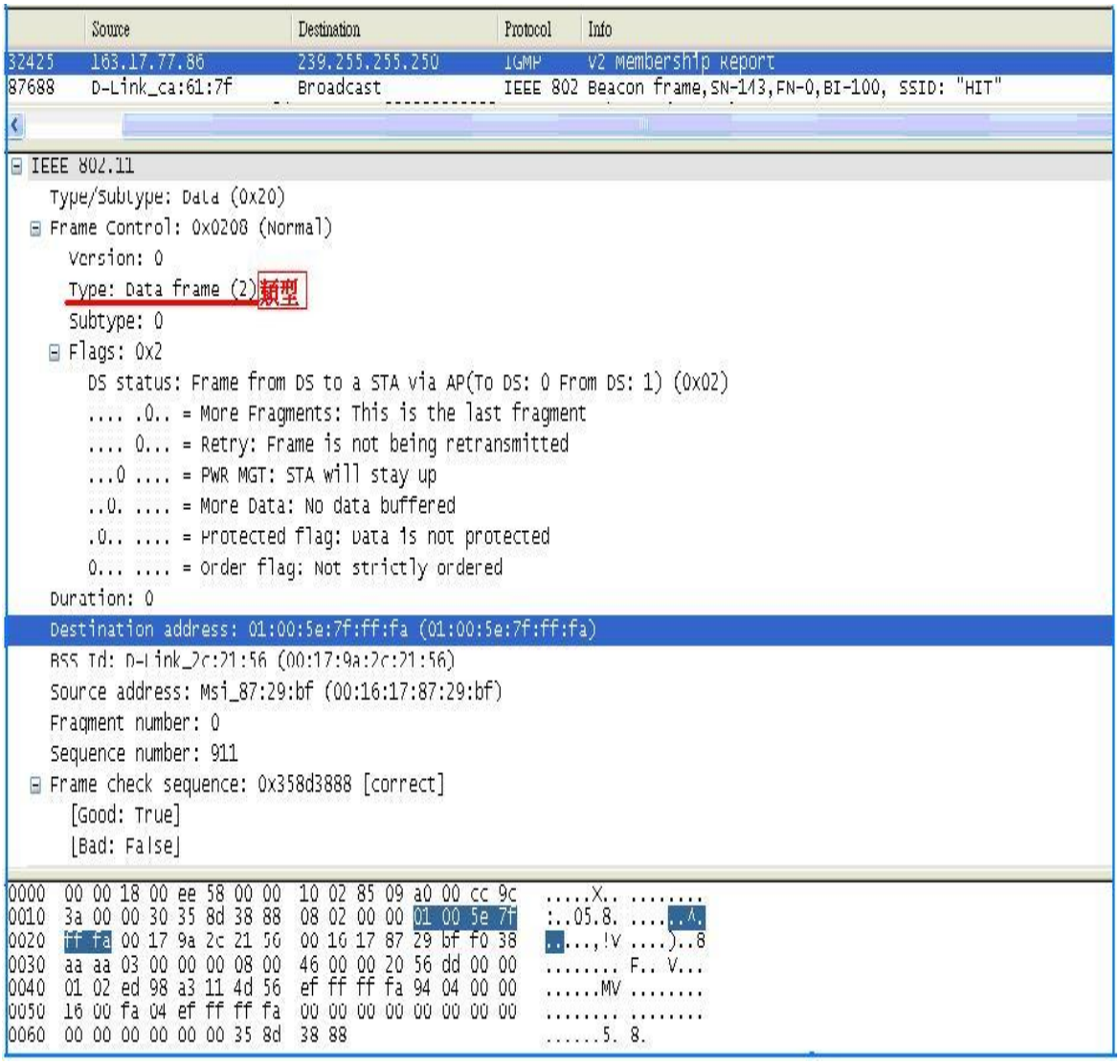


圖 4.2.3 封包資料 IEEE 802.11 欄位- 類型(Type)

子類型(Subtype；4 位元)：(如下圖 4.2.4 所示)

每一種類型訊框還區分為許多不同的子類型(Subtype)，以便更清楚地描述該訊框的種類，如下表

表 1.1 類型與子類型共同紀錄訊框的總類

類型(Type)	訊框類型	子類型(Subtype)	類型種類
00	管理(Management)	1000	Beacon
01	控制(Control)	1011	RTS
01	控制(Control)	1100	CTS
01	控制(Control)	1101	ACK
01	控制(Control)	1110	CF End
10	資料(Data)	0000	Data
10	資料(Data)	1000~1111	保留(Reserved)
11	保留(Reserved)	0000~1111	保留(Reserved)

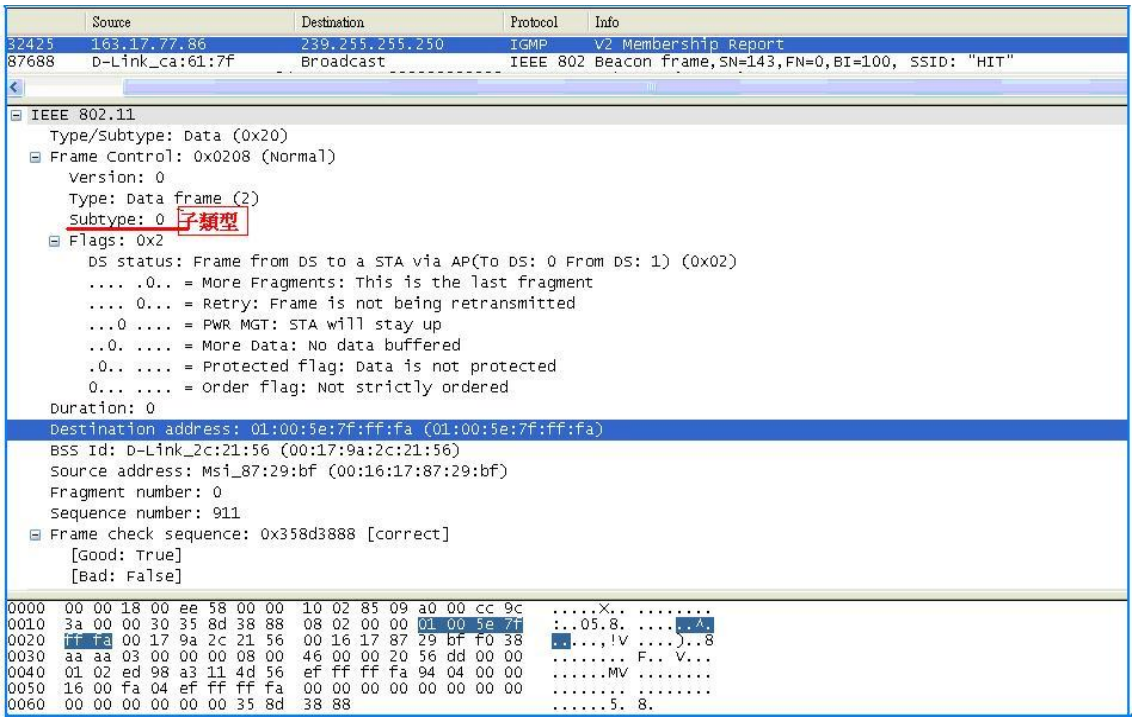


圖 4.2.4 封包資料 IEEE 802.11 欄位- Subtype(子類型)

4.2.2 Frame Control 欄位- Flags(To DS／From DS)介紹

To Ds(To Distribution System；1 位元)：(如下圖 4.2.5 所示)

Ds 就是指分散式系統，也就是讓不同 BSS 間相互溝通的網路系統，To Ds 欄位與 From Ds 一起運用，用以描述此訊框的傳送對象，當 To Ds 欄位為 1 時表示這個訊框是要傳送到一個分散式系統。

From Ds(From Distribution System；1 位元)：(如下圖 4.2.5 所示)

與 To Ds 欄位一起運用，當 From Ds 欄位為 1 時表示這個訊框是從分散式系統傳來的，如下表說明 To Ds、From Ds 兩個欄位在不同組合情況下所代表的意義。

表 1.2 To Ds 與 From Ds 不同組合代表的意義

組　合	意　義
To Ds = 0 ；From Ds = 0	同一個 BSS，由一台主機傳給另一台主機
To Ds = 1 ；From Ds = 0	要傳送到分散式系統的訊框
To Ds = 0 ；From Ds = 1	從分散式系統傳來的訊框
To Ds = 1 ；From Ds = 1	經分散式系統傳到另一個 BSS 內的主機

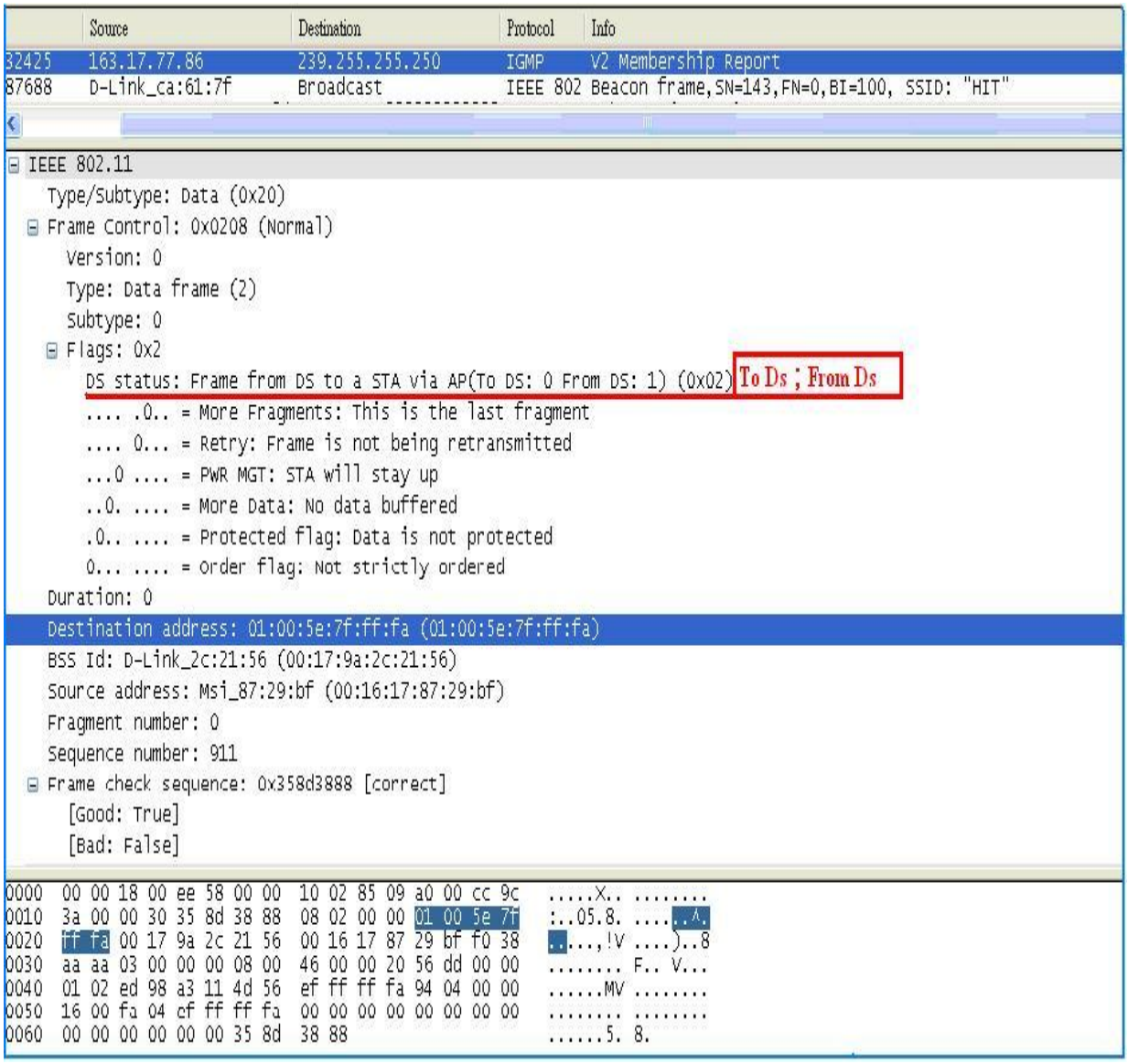


圖 4.2.5 封包資料 IEEE 802.11 欄位- To DS／From DS

其他分段(More Fragment；1 位元)：(如下圖 4.2.6 所示)

訊框的傳送工作有時會因為傳送容量的問題而進行切割，此欄位為 1 時，表示還有其他片段要傳送。

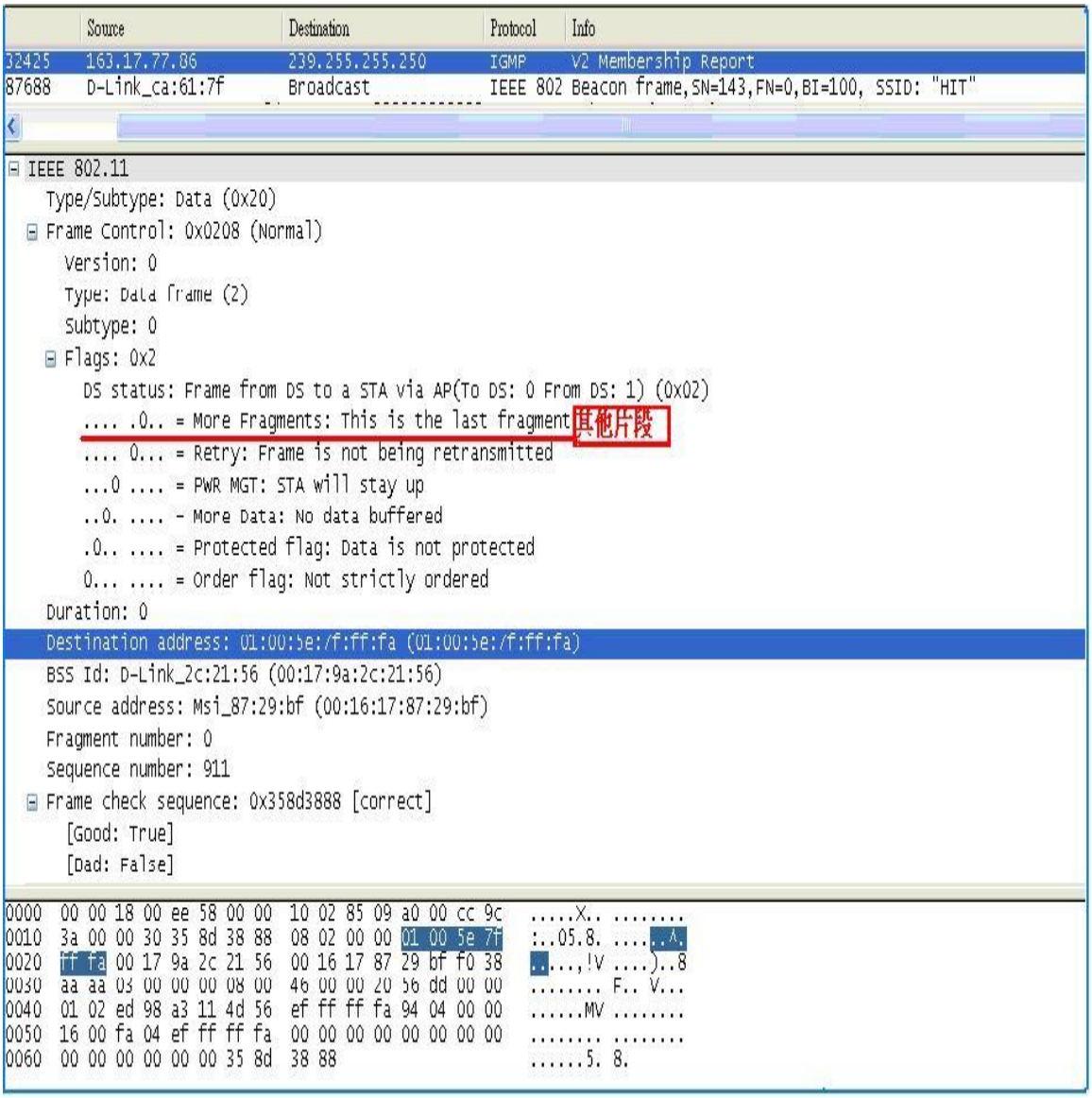


圖 4.2.6 封包資料 IEEE 802.11 欄位- More Fragments(其它分段)

重試(Retry)；1 位元：(如下圖 4.2.7 所示)

當網路發生碰撞或是發送端沒有收到 ACK 訊息的時候，代表此次傳送失敗，必需重送訊框，此時這個欄位會設成 1，表示這個訊框是個重送的重試訊框。

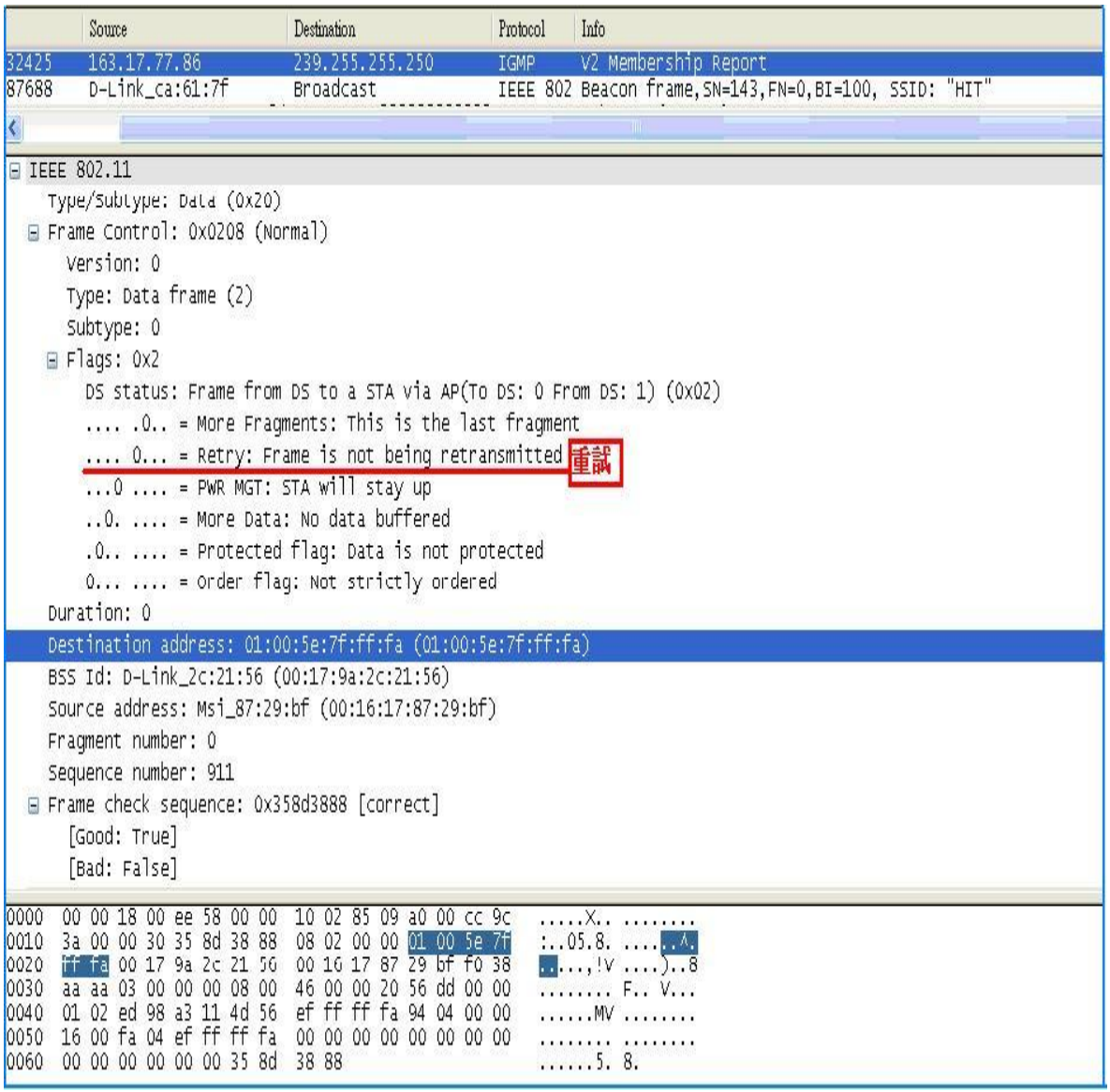


圖 4.2.7 封包資料 IEEE 802.11 欄位- Retry(重試)

電源管理(Power Management；1 位元)：(如下圖 4.2.8 所示)

無線網路的設備因為強調移動性，所以其電源供應不像有線網路設備那麼充裕，所以有效的節省電力一直是無線網路設備重要的課題，而電源管理這個欄位就是用來記錄來源端的電源狀態，當欄位為 1 時，表示此來源端節點處於省電模式，0 則是一般的正常模式。

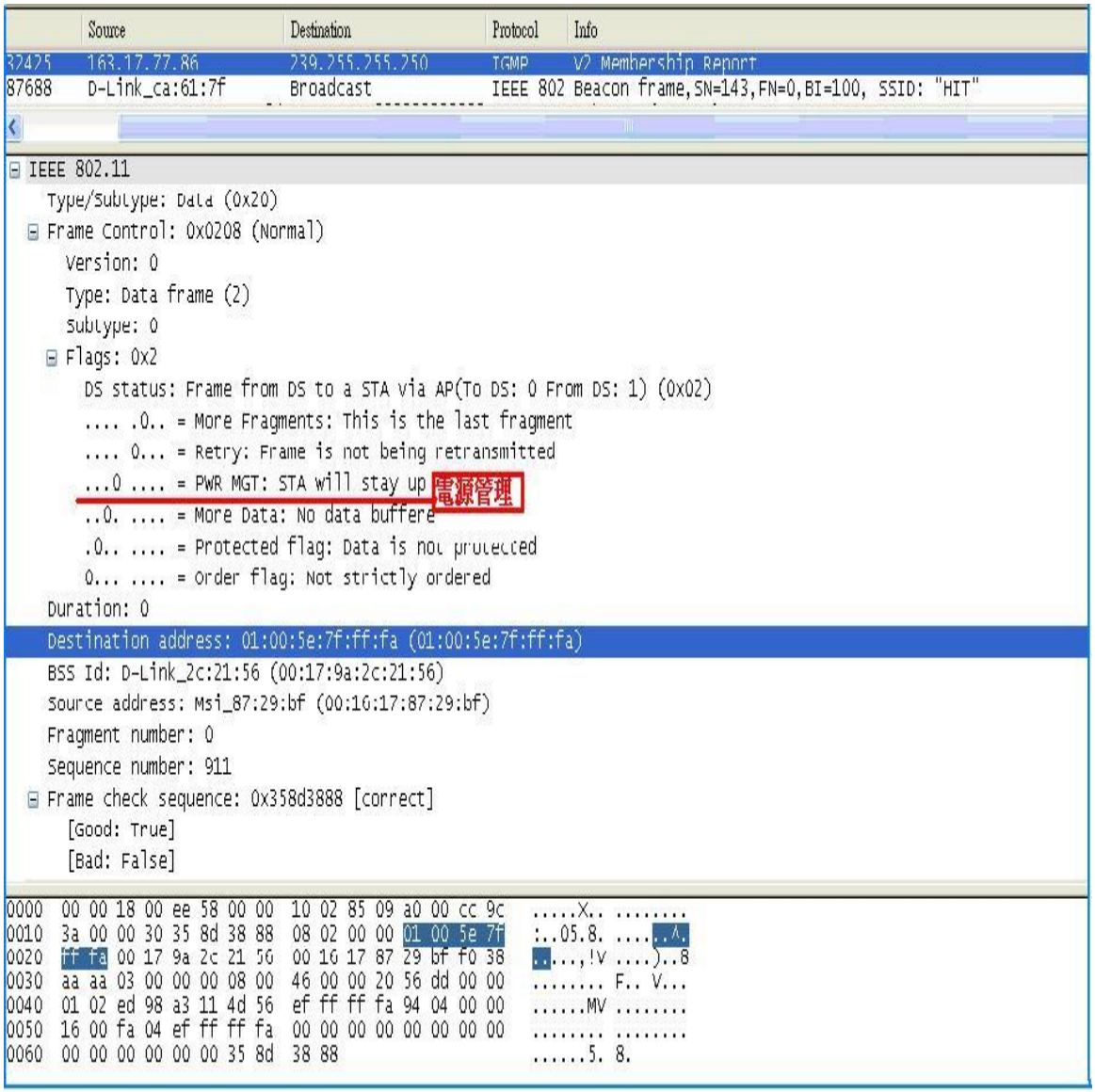


圖 4.2.8 封包資料 IEEE 802.11 欄位- Power Management(電源管理)

其他資料(More Data；1 位元)：(如下圖 4.2.9 所示)

此位元為 AP 用來告訴省電模式中的接收端主機資料是否已經傳送完畢？一般的情況下，欄位值為 0，表示此份資料已經傳送結束，當欄位值為 1 時，表示資料尚未完全傳送完成。

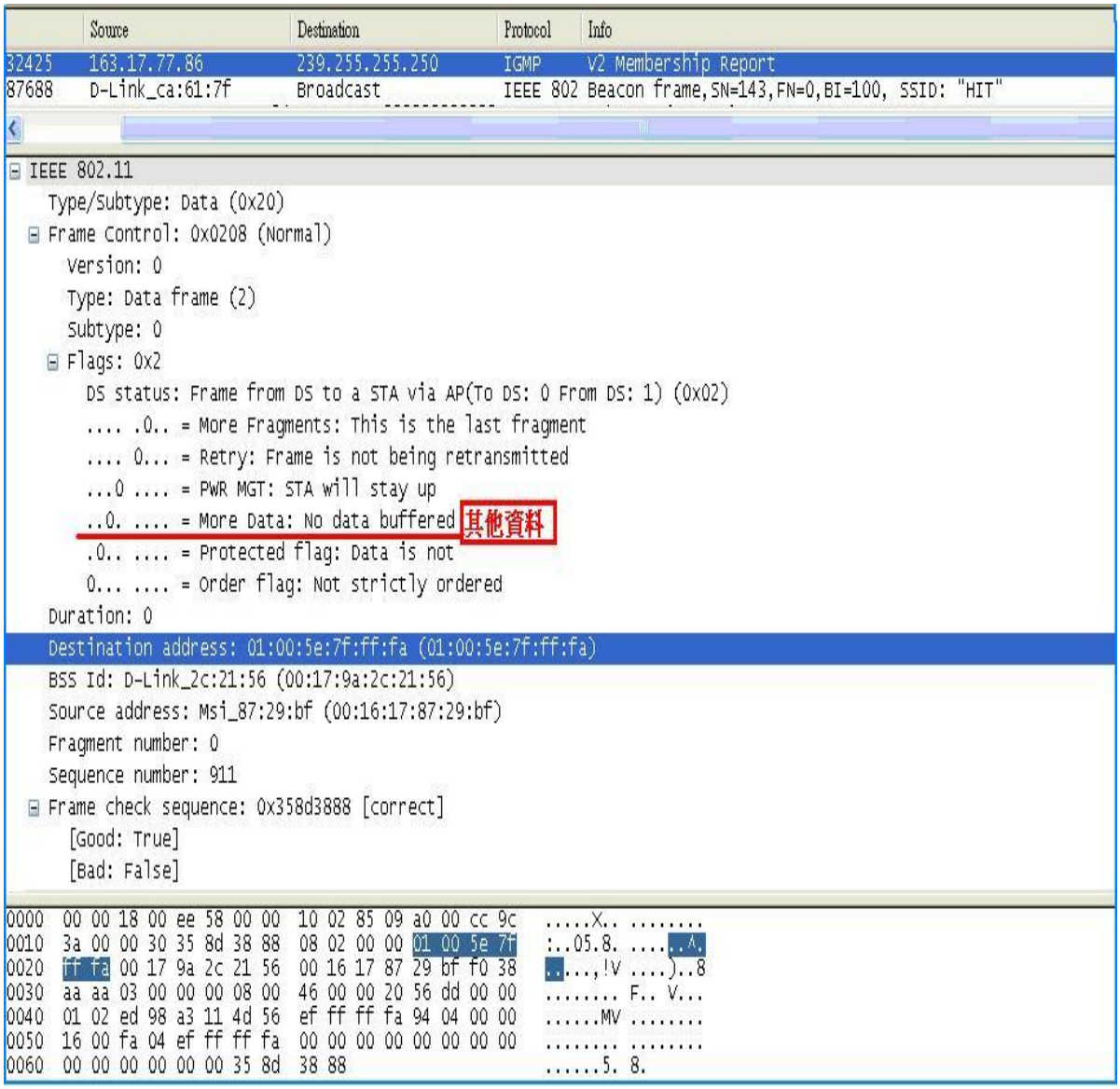


圖 4.2.9 封包資料 IEEE 802.11 欄位- More Data(其它資料)

WEP(Wired Equivatent Privacy；等效於有線的保密機制；1 位元)：(如下圖 4.2.10 所示)

WEP 是 802.11 機制為避免訊號在無遮掩的無線傳播環境中遭到竊取所建置的保密機制，此欄位為 1 時，表示此資料訊框經過 WEP 機制加密處理過，否則表示該訊框未經加密處理。

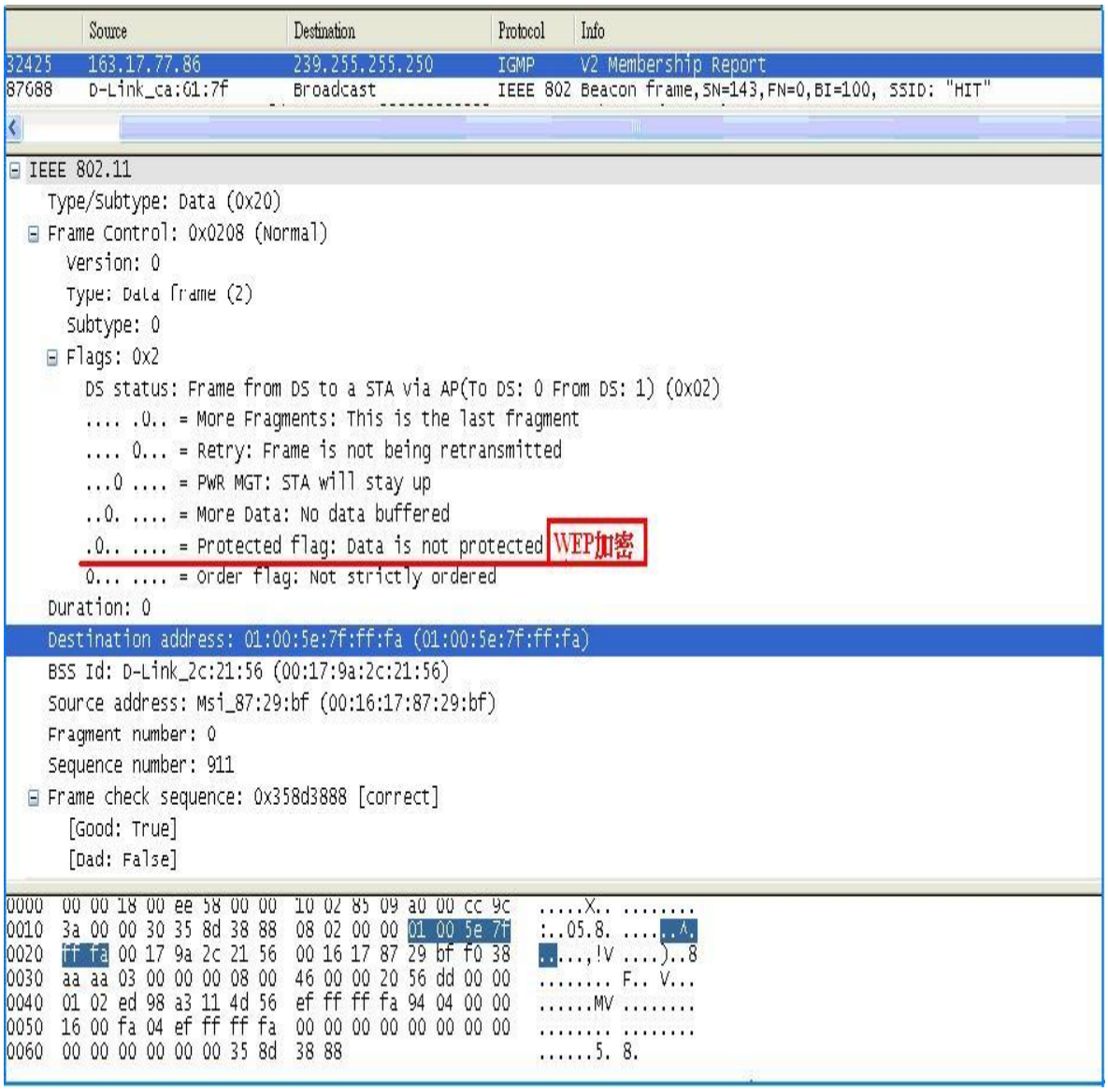


圖 4.2.10 封包資料 IEEE 802.11 欄位- Protevted flag(WEP 加密)

Order(1 位元)：(如下圖 4.2.11 所示)

欄位值為 1 表示此訊框是經由嚴格依序服務等級(Strictly Ordered Service Class)進行傳送，所謂嚴格依序服務等級就是訊框是按照順序來傳送，不過大部分的情況這個欄位值會設為 0，也就是不強制要按照順序來進行訊框的傳送，由接收端運用訊框標頭內的序列控制欄位值進行重組。

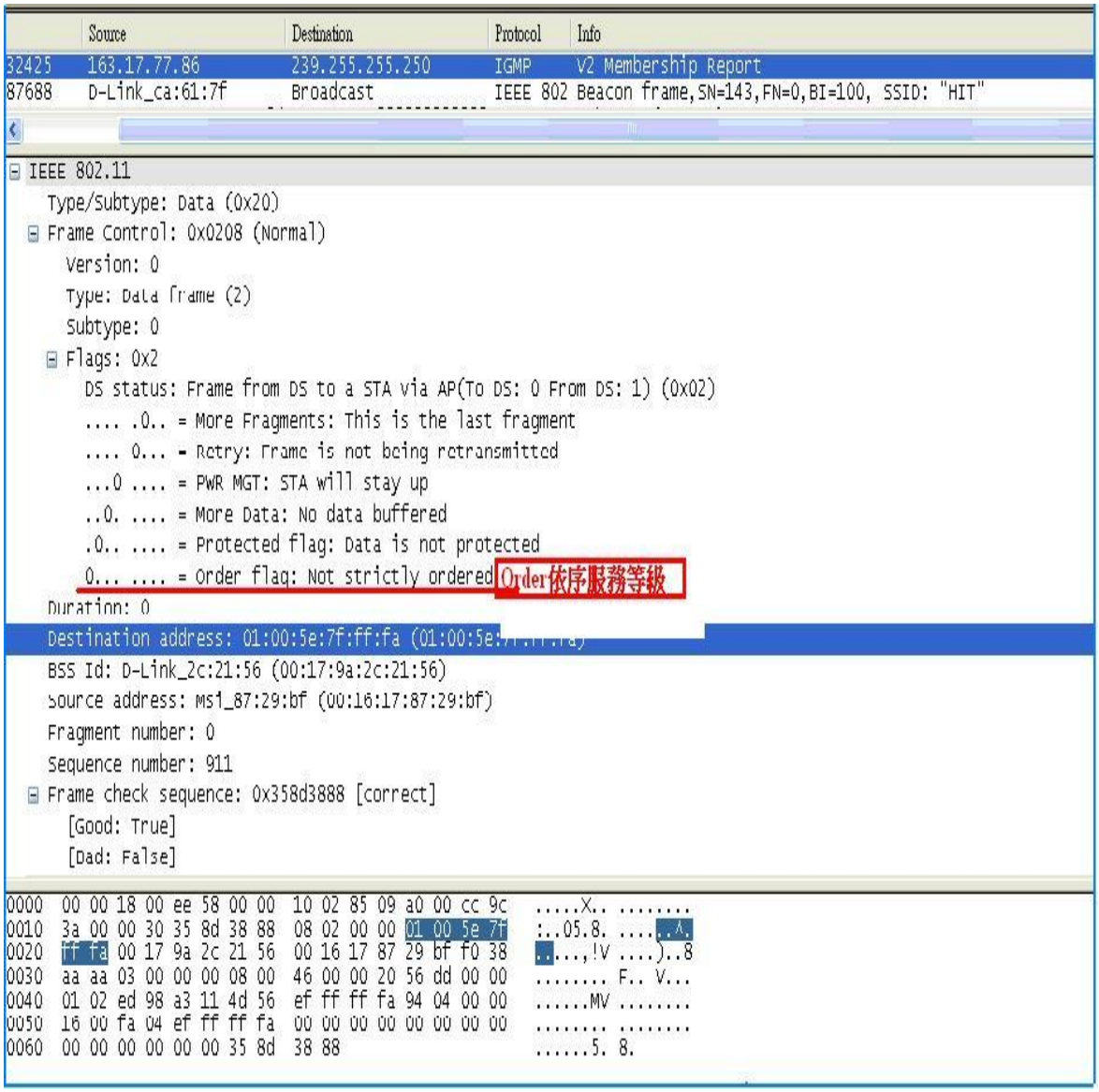


圖 4.2.11 封包資料 IEEE 802.11 欄位- Order**(**順序（服務等級）**)**

4.2.3 Frame Control 欄位- Duration、位址、序列控制介紹

持續時間/識別碼(Duration/ID;；2 位元組)：(如下圖 4.2.12 所示)

這個欄位依數值的不同如下表所示有不同的用途，有些區塊暫時保留(Reserved)尚未定義，其他則主要提供傳送預計持續的時間或工作站 ID 使用。 當欄位值小於 32768 時，這個欄位用來記錄主機需多少時間來進行資料的傳送工作，時間以微秒為單位，收到訊號的主機可以根據此持續時間訊息進行虛擬載波的偵測； 數值等於 32768 時，表示傳送工作處在免競爭週期內，傳送以輪詢方式進行； 至於數值大於 32768 時，大部分屬於保留區塊，只有一小部分數值提供在省電模式中對工作站進行辨識的辨識碼(ID)使用。

表 1.3 Duration／ID 欄位中數值代表的時間

第 15 個位元	第 14 個位元	第 13~0 個位元	用途
0	0~32767		持續時間
1	0	0	免競爭週期
1	0	1~16383	保留
1	1	0	保留
1	1	1~2007	紀錄工作站的 ID
1	1	2008~16383	保留

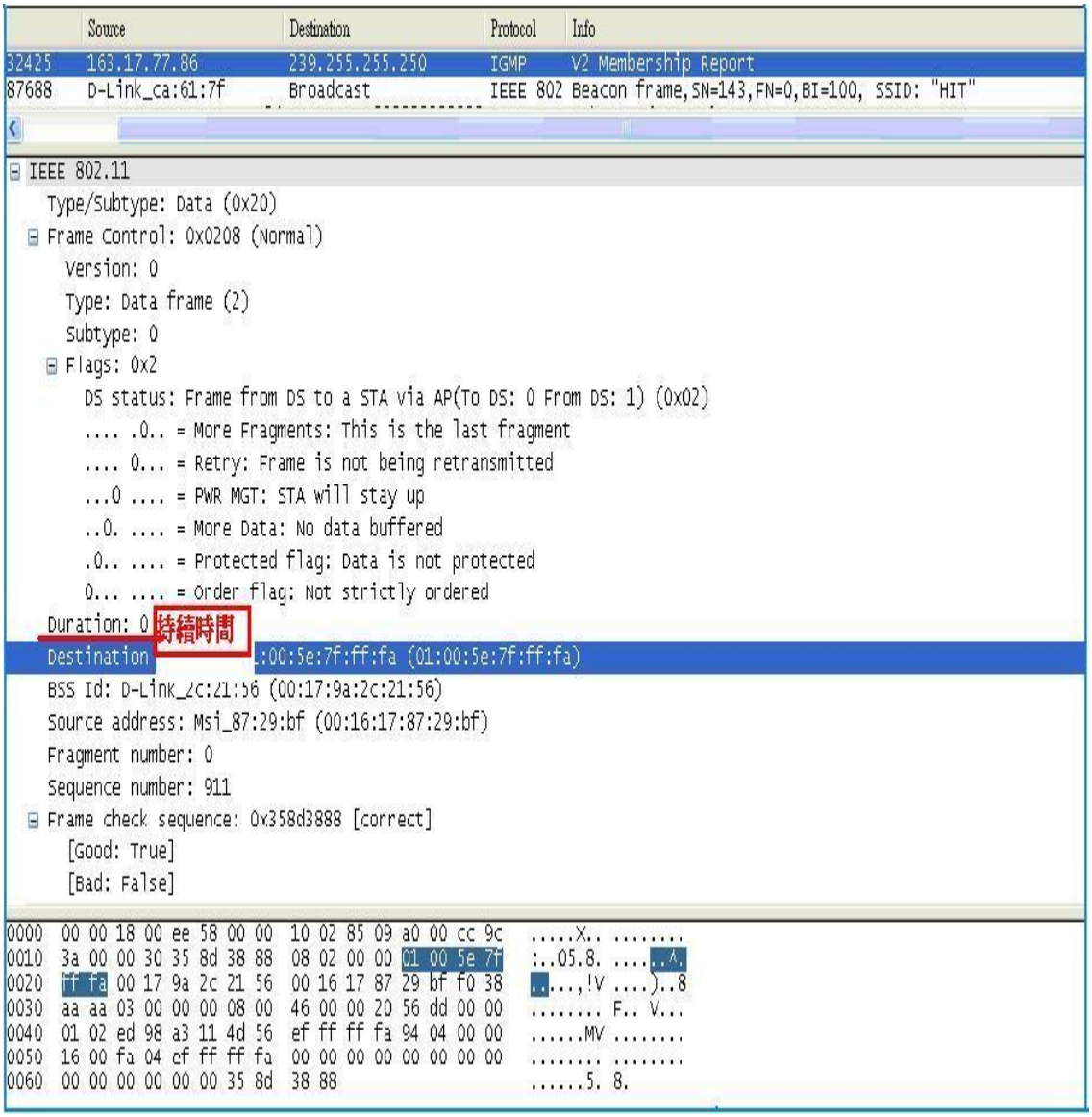


圖 4.2.12 封包資料 IEEE 802.11 欄位- Duration(持續時間)

位址欄位(Address；6 位元組)：(如下圖 4.2.13 所示)

802.11 標頭內有 4 個 MAC 位址欄位，各佔 6 個位元組，用以根據不同用途紀錄各種不同的 MAC 位址。4 個 MAC 位址欄位如下表所示與 To Ds 與 From Ds 一起搭配，有各種不同的配置(如下表)，位址的類型大約有五類，分別是來源端位址(SA：Source Address)、目的端位址(DA：Destination Address)、傳送資料位址(TA：Transmitter Address)、接收資料位址(RA：Receiver Address)以及 BSSID(BSS Identifier)；其中傳送資料與接收資料的位址通常是作為中介 AP 的 MAC 位址。

表 1.4 不同 To Ds 與 From Ds 搭配的位址欄位內容

To Ds	From Ds	位址 1	位址 2	位址 3	位址 4
0	0	DA	SA	BSSID	不使用
0	1	DA	BSSID	SA	不使用
1	0	BSSID	SA	DA	不使用
1	1	RA	TA	DA	SA

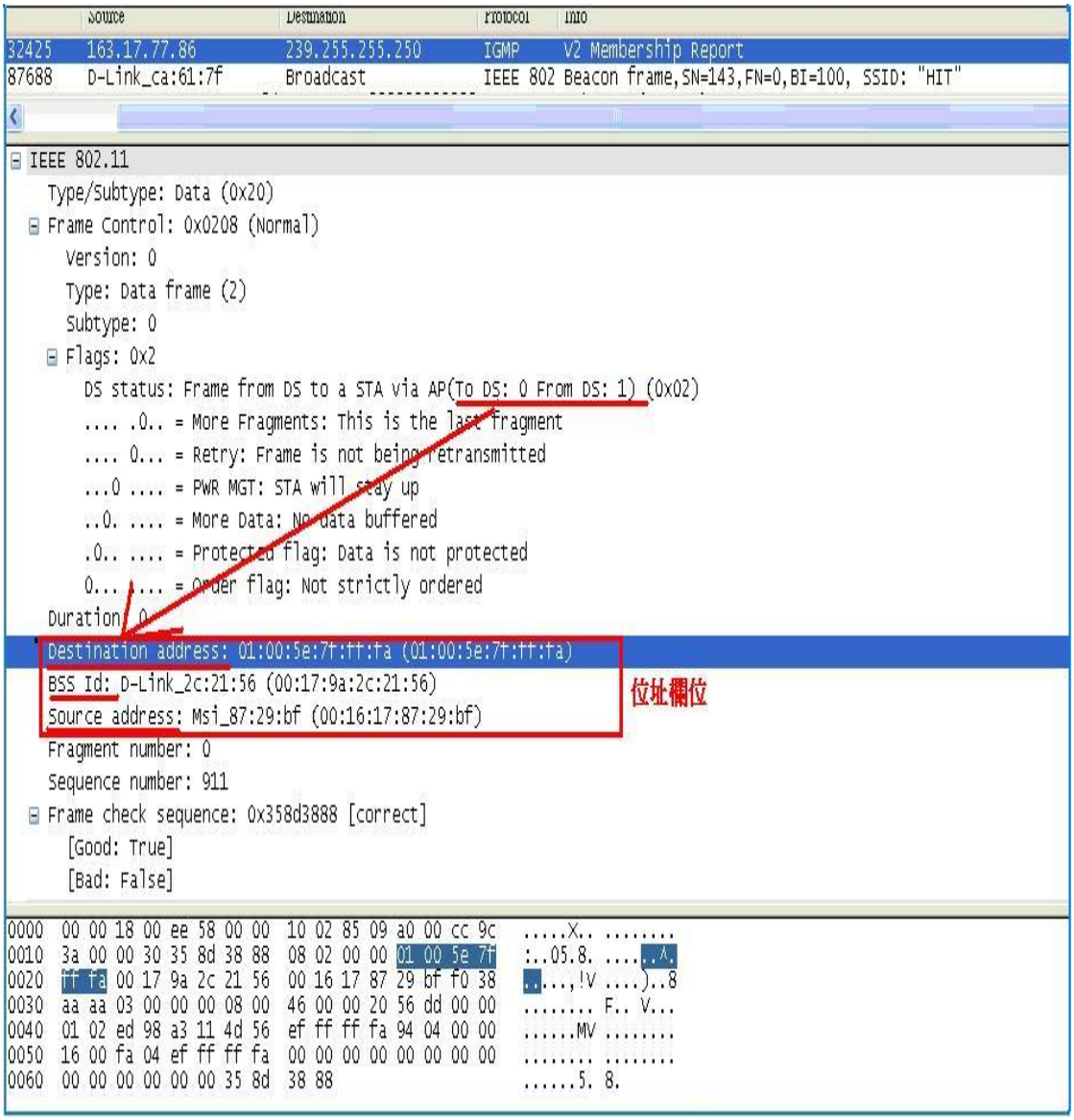


圖 4.2.13 封包資料 IEEE 802.11 欄位- 位址欄位 address

序列控制(Sequence Control；2 位元組)：(如下圖 4.2.14 所示)

序列控制欄位主要對訊框的次序進行紀錄，其下又分有兩個次欄位，分別是 12 個位元的序列號碼(Sequence Number)與 4 個位元的片段號碼(Segment Number)。

一般情況，並沒有對訊框進行切割，因此都只用到第一個次欄位的部份，至於第二個部份的片段號碼，在訊框進行切割時才會用到，以便接收端可以根據這些的片段號碼將訊框正確組合回來。

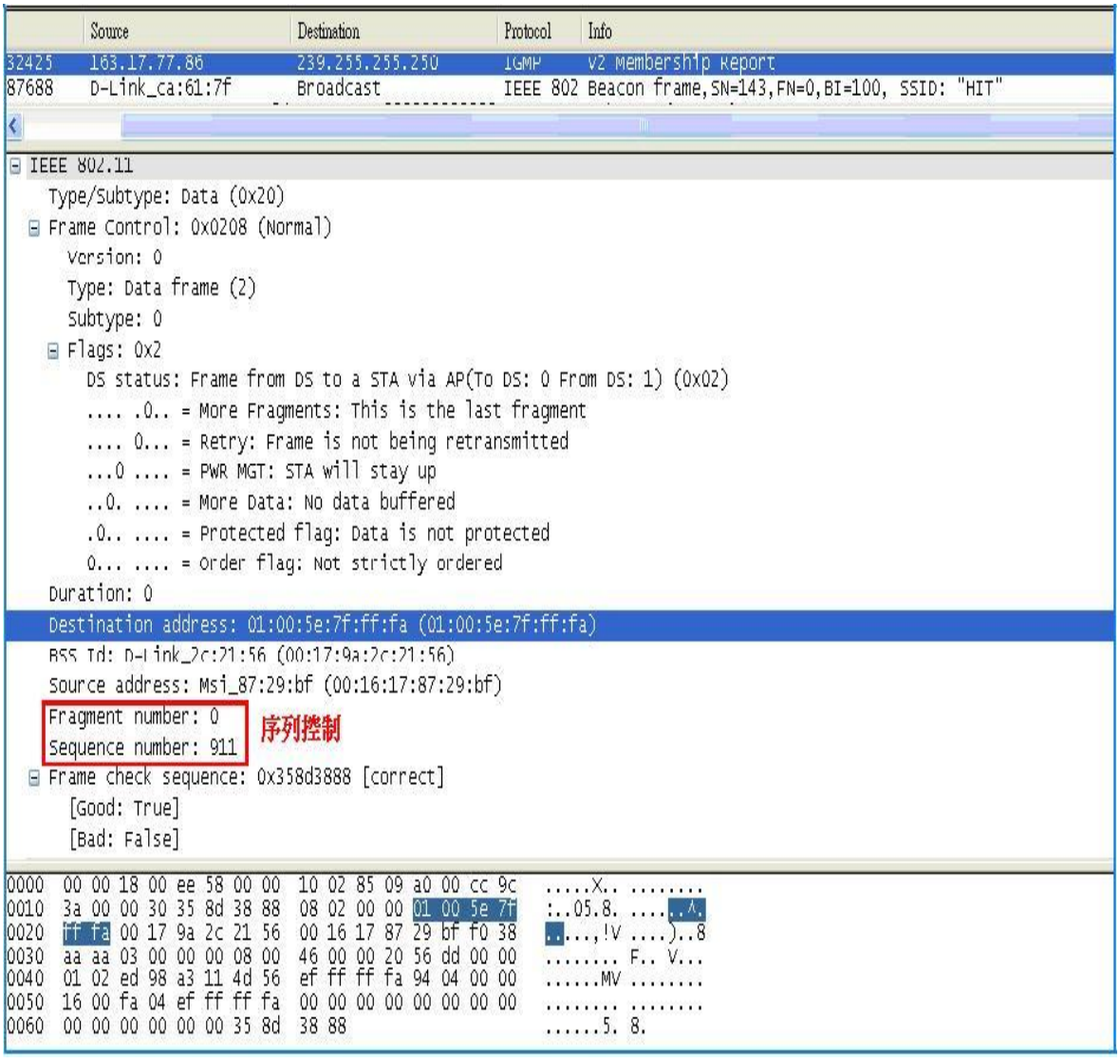


圖 4.2.14 封包資料 IEEE 802.11 欄位- 序列控制

4.2.4 其它介紹

資料區段(Data；<2312 位元組)

記錄所攜帶的資料，以位元組為單位，最大不可超過 2312 個位元組，資料欄位內容也包含了 LLC 子層 802.2 及其他層級協定的標頭資訊。

檢查碼(4 位元組)：(如下圖 4.2.15 所示)

佔 4 個位元組，以 CRC-32 方式對資料訊框進行錯誤的檢測。

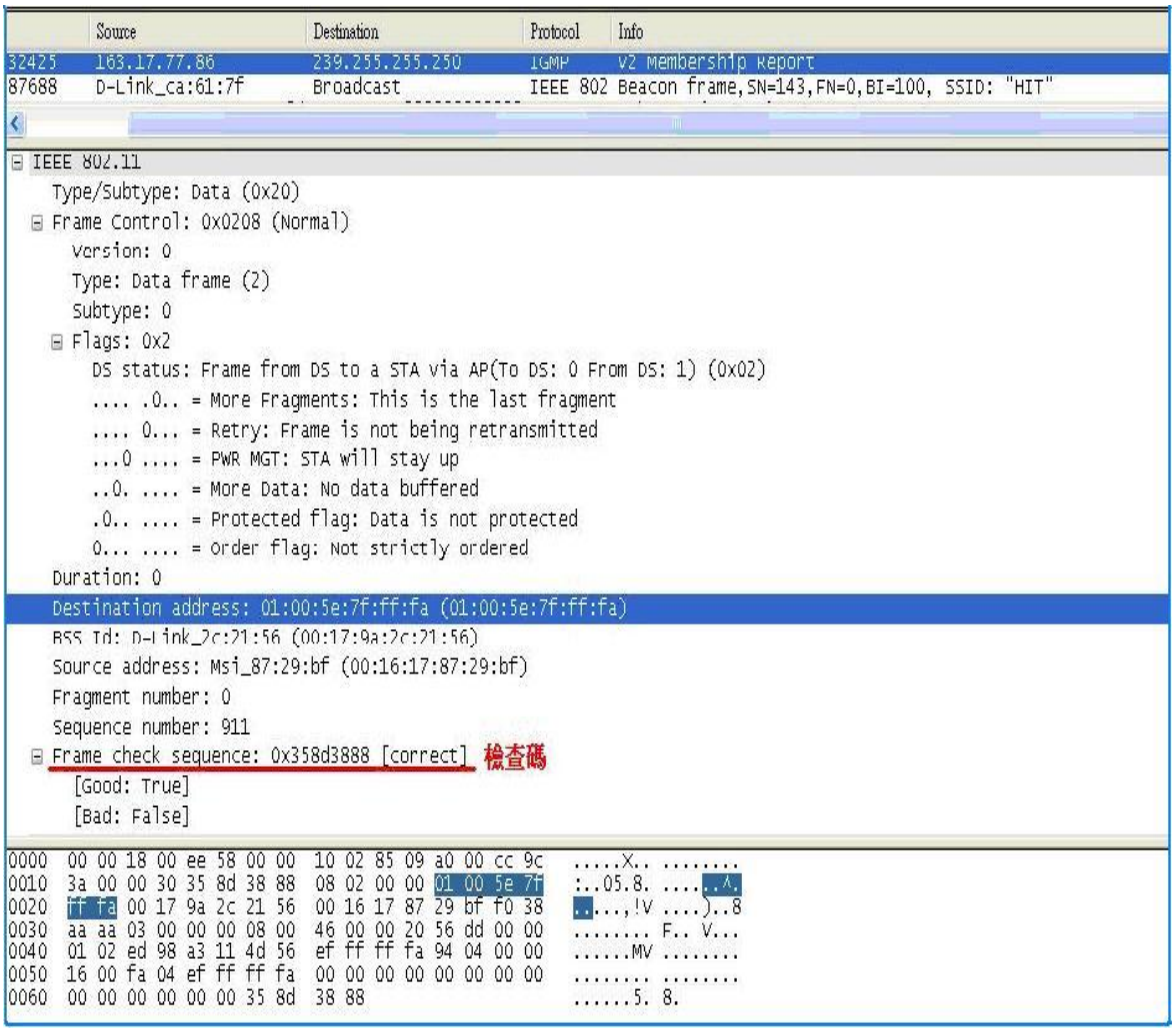


圖 4.2.15 封包資料 IEEE 802.11 欄位- 檢查碼

4.3 IEEE 802.11－MAC 層協定

802.11 規格主要涵蓋在 OSI 實體層與 MAC 子層的部分，而其 MAC 子層的處理方式又區分為兩種，一個市集中式協調功能(PCF；Point Coordination Function)的方式，另一個則是分散式協調功能(DCF；Distributed Coordination Function)的方式。

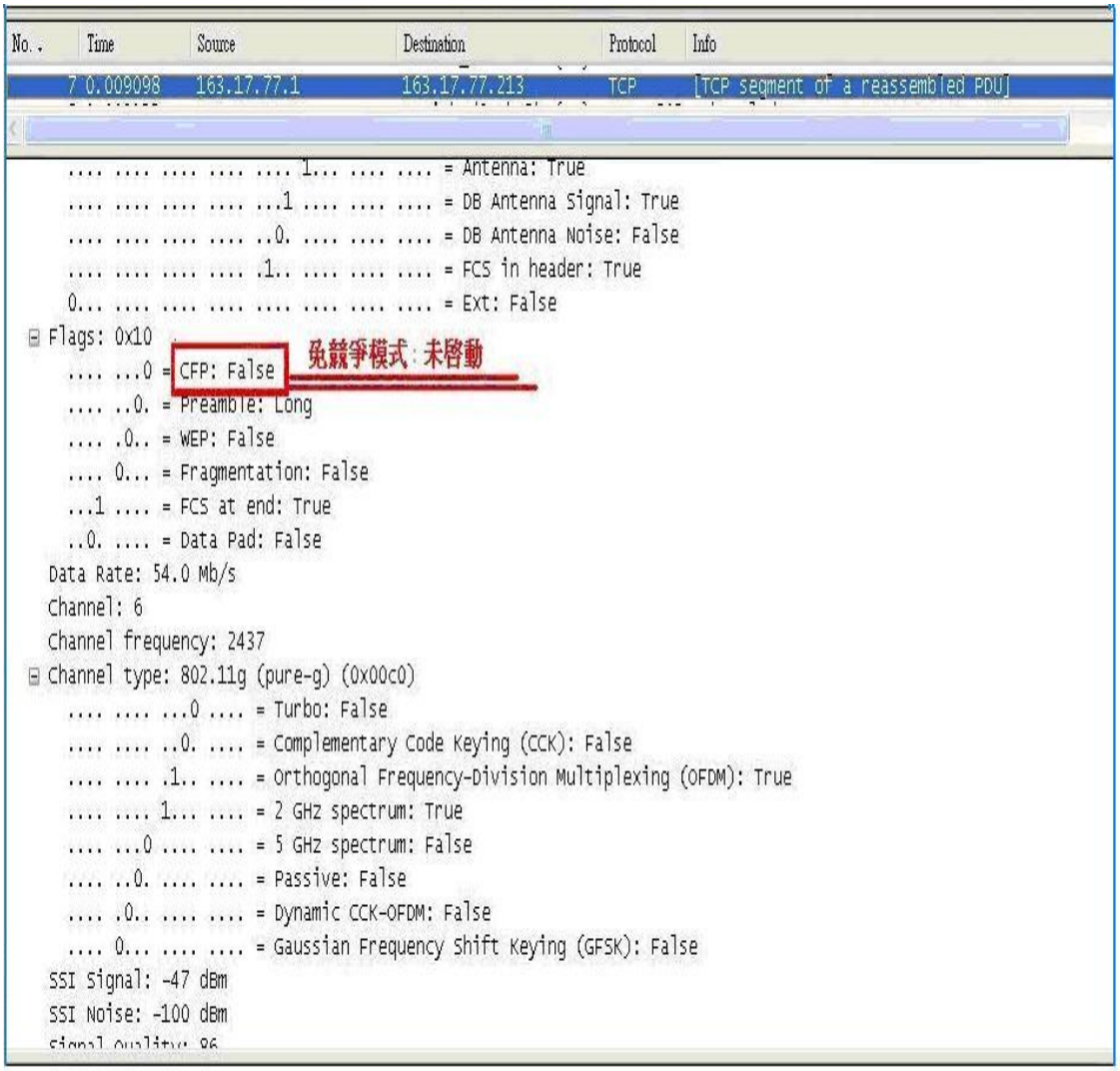


圖 4.3.1 免競爭模式-有/無啟動查詢

集中式協調功能(PCF)，扮演集中協調者的角色，由協調者輪流詢問(Polling)各主機是否要發言，只有被詢問到的主機才有機會發言；協調者通常由 AP 來擔任，因此 PCF 架構通常只適用在 Infrastructure 無線環境中。PCF 架構的主控權在協調者身上，各主機間並不具競爭性，因此屬於免競爭式(Contention Free)的傳送，也不會有碰撞發生。

至於分散式協調功能(DCF)由要發送訊息的主機互相去爭取發送權，屬於競爭式(Contention)的傳送機制。無論是 Ad hoc 或 Infrastructure 環境，每一個無線主機都具備這個功能，其工作原理就是運用 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance；載波感測多重存取/碰撞避免)進行通訊工作的授權。

免競爭傳輸模式

PCF 免競爭的運作流程如下圖 4.3.2 所示，在還沒正式進入免競爭周期之前，協調者會先偵測網路上是否已經有資料正在傳送，如果沒有則等待過一個訊框間隔(稱之為 PIFS；PCF inter-Frame Space)後，如果確定網路上真的沒有訊號在進行傳送，協調者便會送出一個烽火訊框(Beacon)來啟動免競爭週期，由協調者取得網路的使用權，其他節點則必須將等待傳送時間的值設成免競爭的最大週期值，以避免各節點在免競爭週期內自行將資料送出所發生錯誤。

進入免競爭周期之後，協調者開始根據輪詢名單輪流詢問各加入輪詢的主機是否要傳送資料，最後當輪詢名單空白豁免競爭週期時間到，協調者會送出一個免競爭結束(CF-End；Contention Free End)控制訊框，已結束此次免競爭週期，並進入另一次的競爭週期。

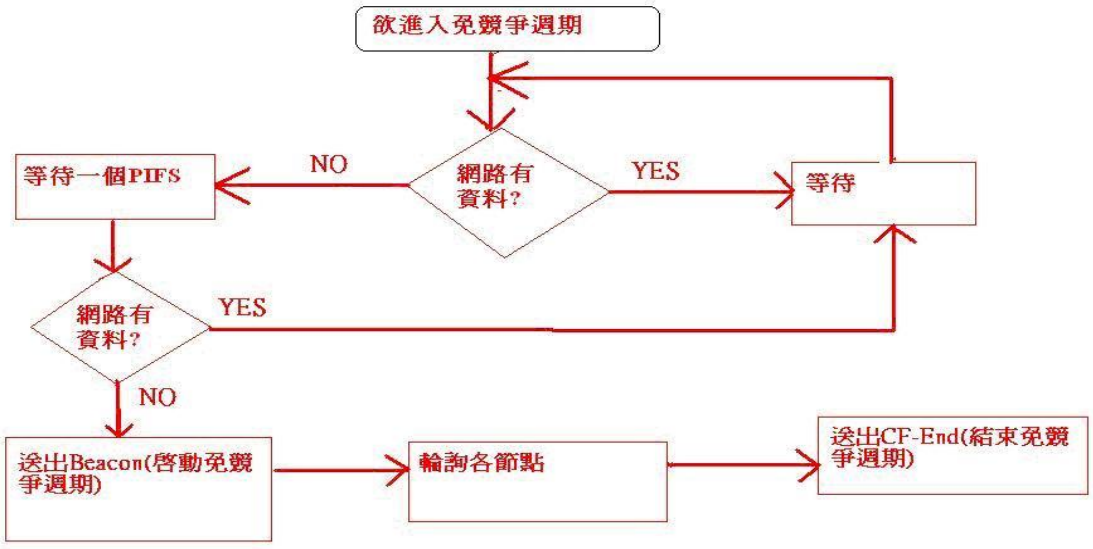


圖 4.3.2 集中式協調 PCF(免競爭) 運作流程

4.4 CSMA/CA 運作流程

4.4.1 DCF_CSMA／CA 機制：分散式協調功能（競爭模式）

1.如圖 4.4.1，先偵測所使用的網路是否有別人在使用。偵測期間需為 DIFS 時間加上一個亂數時間，若沒人使用則繼續下一步。

2.傳送端送出 RTS 封包給接收端，告訴對方想要傳送資料。

3.接收端收到 RTS 封包後，會在 SIFS（Short IFS）時間內回應 CTS（Clear To Send）封包給傳送端。

4.傳送端收到 CTS 封包後，會開始傳送資料。

5.接收端收到資料會回應 ACK(Acknowledge)封包進行確認；若傳送端未收到 ACK 封包，就判定傳送失敗，回到第一步重新開始。

4.4.2 PCF_CSMA／CA 機制：集中協調功能（免競爭模式）

1.進入 CF 模式時，AP 會在 Beacon 封包中加入使用 CF 模式的時間。各站台收到些封包，會將此加入他們的等待時間。

2.AP 開始依照內部清單的順序，用[CF-Poll]封包輪流詢問各站台是否要傳送資料。如果在詢問時，恰好有資料要傳給該節點，AP 會將資料連同詢問一起送出，稱為[Data+CF=Poll]封包。

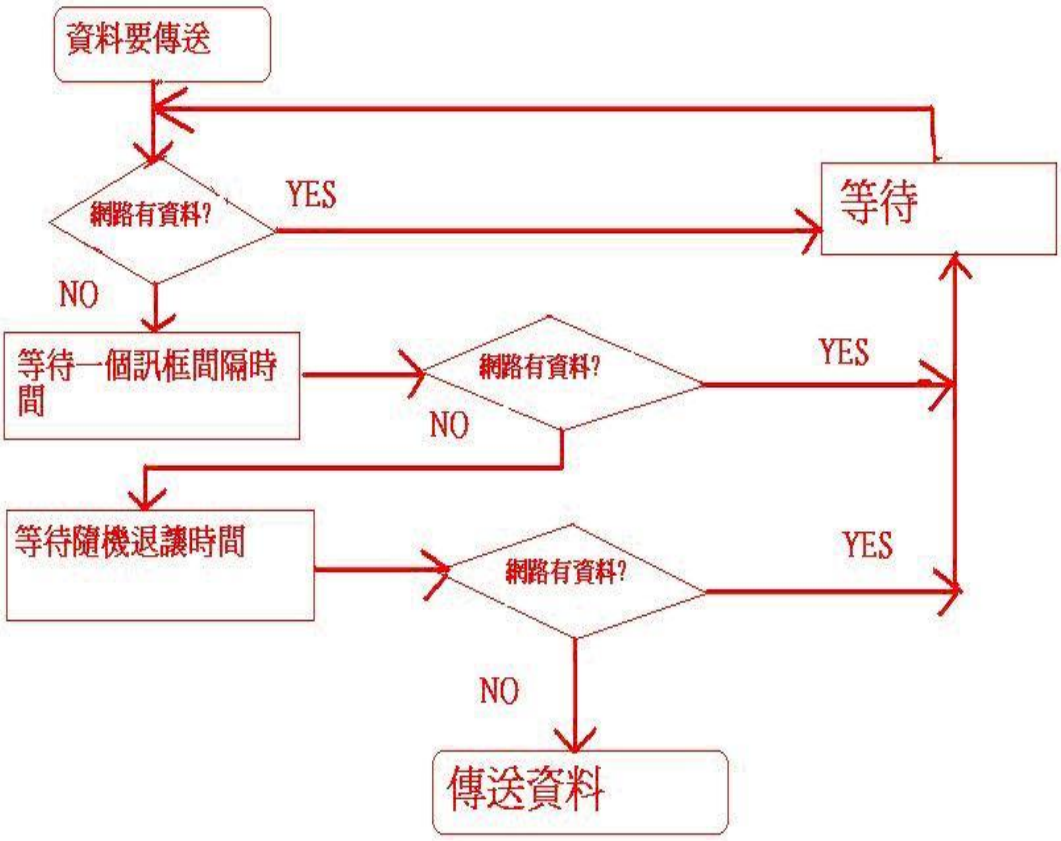


圖 4.4.1 CSMA/CA 運作流程

IEEE802.11 的訊框間隔時間因為訊框類型的不同有幾種形式，重要性越高的訊框類型，所設定的間隔時間會越短，以下是 IEEE802.11 機制下所定義的幾種間隔時間：

1. SIFS (Short IFS)：

短的訊框間隔，用來做立即性的回應，主要用在一些如要求傳送訊框(RTS；Request To Send)、允許傳送訊框(CTS；Clear To Send)、回應訊框(ACK；Acknowledgement)等控制類型訊框傳送錢所需等待的時間；此類型訊框由於具有比較高的重要性，因此所設定的時間最短。

2. PIFS (PCF IFS)：

這是在使用 PCF 傳送方式時，主機傳送訊息前所需等待的時間。

3. DIFS (DCF IFS)：

是運用 DCF 傳送方式時，主機傳送訊息前所要等待的時間。

4. EIFS (Extended IFS)：

主機在進行崇送訊框時所需等待的時間。

四種訊框間隔的時間長短大致為 SIFS> PIFS>DIFS>EIFS，間隔時間越短，因為等待的時間短，使用傳輸媒介的機率會越大，也就會分配給優先權高的訊框使用。下表列出四種訊框間隔的優先權及其用途，訊框間隔時間依系統實體層的特性不同有不同的設定，但差距以各自設定的時槽時間(SlotTime)為間隔；以 802.11b/g 與 802.11a 的情況為例，SIFS 時間分別為 10us 與 16us，而各訊框間隔差距的時槽時間分別訂為 20us 與 9us，因此兩種架構的 PIFS 分別為 30us 與 25us。

表 1.5 訊框間隔與優先權

訊框間隔	802.11a	802.11b/g	用途	優先權
SIFS	16	10	RTS、CTS、ACK	最高
PIFS	25	30	PCF 傳送模式	第二
DIFS	34	50	DCF 傳送模式	第三
EIFS	43	70	重送訊框	最低

為了要能避免碰撞的發生，CSMA/CA 再運用所謂的退讓時間(Backoff Time)來進行等待，退讓時間由亂數隨機產生，以避免產生相同的退讓時間，但如果真的產生相同的退讓時間導致碰撞的發生，傳送工作就只好再重新來過了。

退讓時間的計算也以時槽時間(Slot Tine)為單位，選取的亂數範圍值稱為競爭視窗(CW；Contention Windows)，競爭視窗如下表所示，依系統實體層的不同與重傳次數有不同的設定，802.11b/g 及 802.11a 的範圍值不同，重傳次數越多，代表網路擁塞的情況越嚴重，訂定的亂數範圍也會越大。

表 1.6 重傳次數與競爭視窗範圍值的關係

情況	802.11b/g	802.11a
初始值	0~31	0~15
第一次重傳	0~63	0~31
第二次重傳	0~127	0~63
第三次重傳	0~255	0~127
第四次重傳	0~511	0~255
第五次重傳	0~1023	0~511
第五次以上重傳	0~1023	0~1023

4.5 To DS／From DS 封包介紹

如下圖所示，要查詢 To DS／From DS 相關訊息，點選 Source 來源端(傳送端)與 Destination 目的端(接收端)這兩個欄位的 IP 位址後(如～圖中標示 1)，在視窗下方依序展開 IEEE 802.11 之中的 Flags 資料進行查看(如～圖中標示 2)。

在最下面的數字資料，都以十六進制表示法所列出來，點選 Flags 資料可看到下面的資料顯示為 $02_{(16)}$ (如～圖中標示 3)，為二進制的 $0000\ 0010_{(2)}$，反過來後的 0100 0000 左邊第一個數值代表 To DS：0、第二個數值代表 From DS：1，對照中間的資料可得到同樣的結果(如～圖中標示 2)。

＊其中 To DS：0／From DS：1 所代表的意思是從分散式系統傳來的訊框。

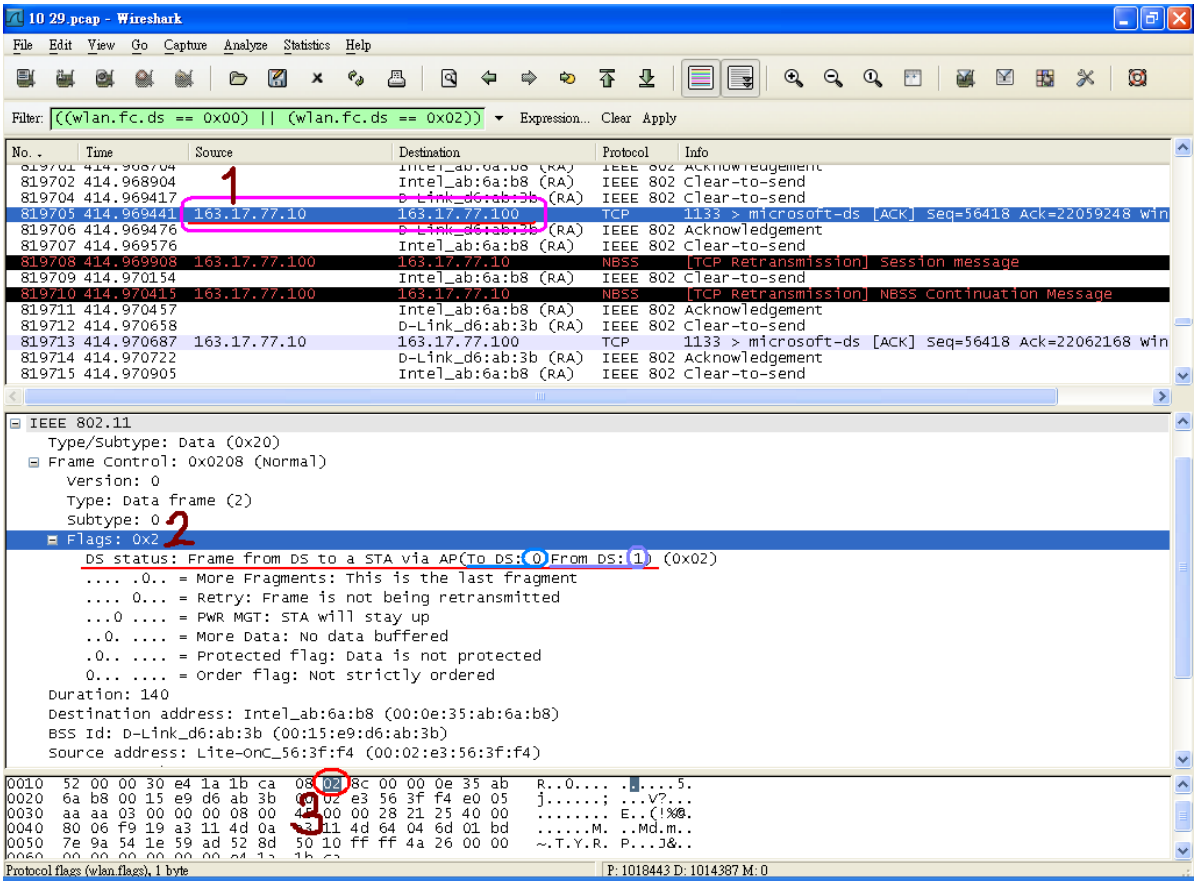


圖 4.5.1 封包資料 To DS／From DS 訊框

在擷取到的封包內容裡，TO DS 與 FROM DS 的值，各有不同的位址內容互相對應，以下將以圖解作介紹

(a) TO DS=1, FROM DS=0 時，代表是一個要傳送到分散式系統的訊框。而位址 1~4 的內容分別為

位址 1：BSSID

位址 2：SA(來源端位址)

位址 3：DA(目的端位址)

位址 4：不使用

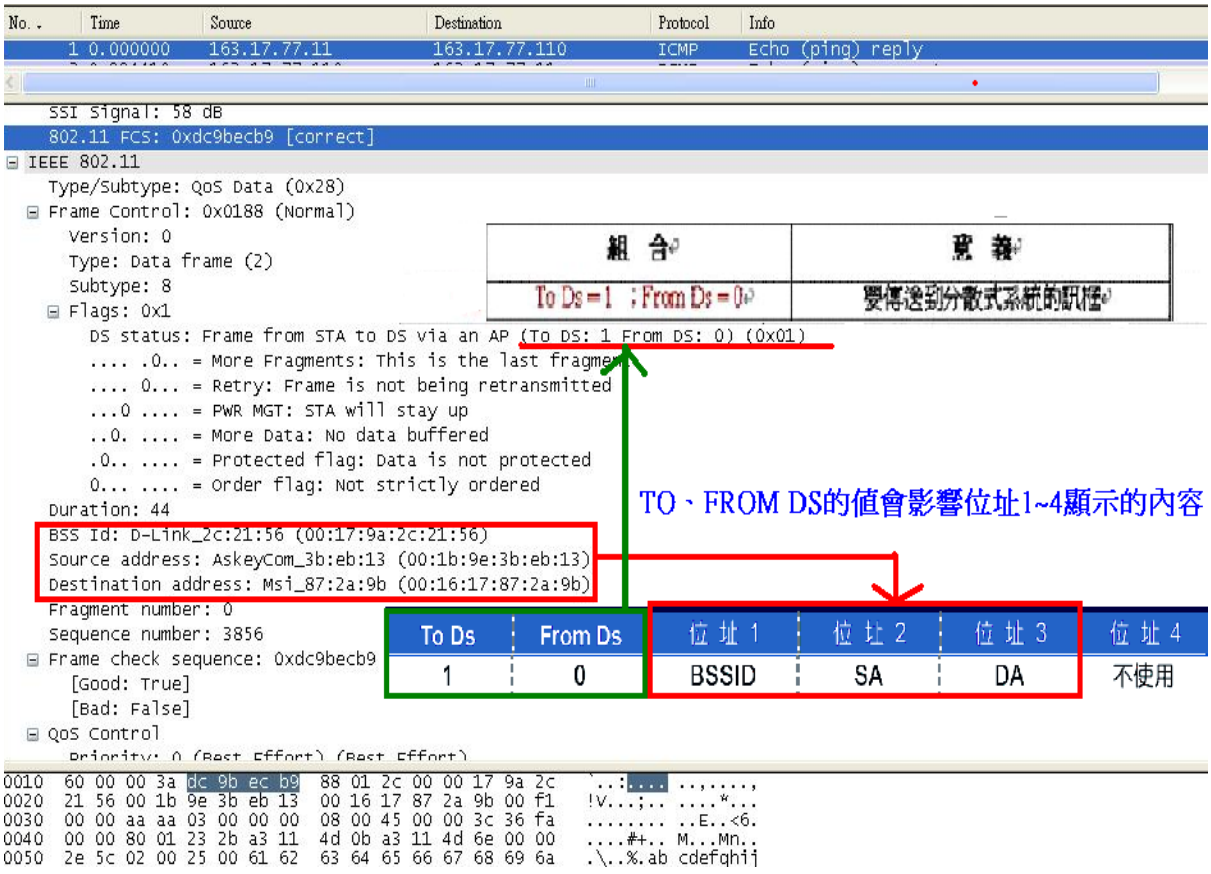


圖 4.5.2 封包資料 To DS =**1**／ From DS = **0** 訊框

(b) TO DS=0, FROM DS=1 時，代表是一個從分散式系統傳來的訊框。而位址 1~4 的內容分別為

位址 1：DA(目的端位址)

位址 2：BSSID

位址 3：SA(來源端位址)

位址 4：不使用

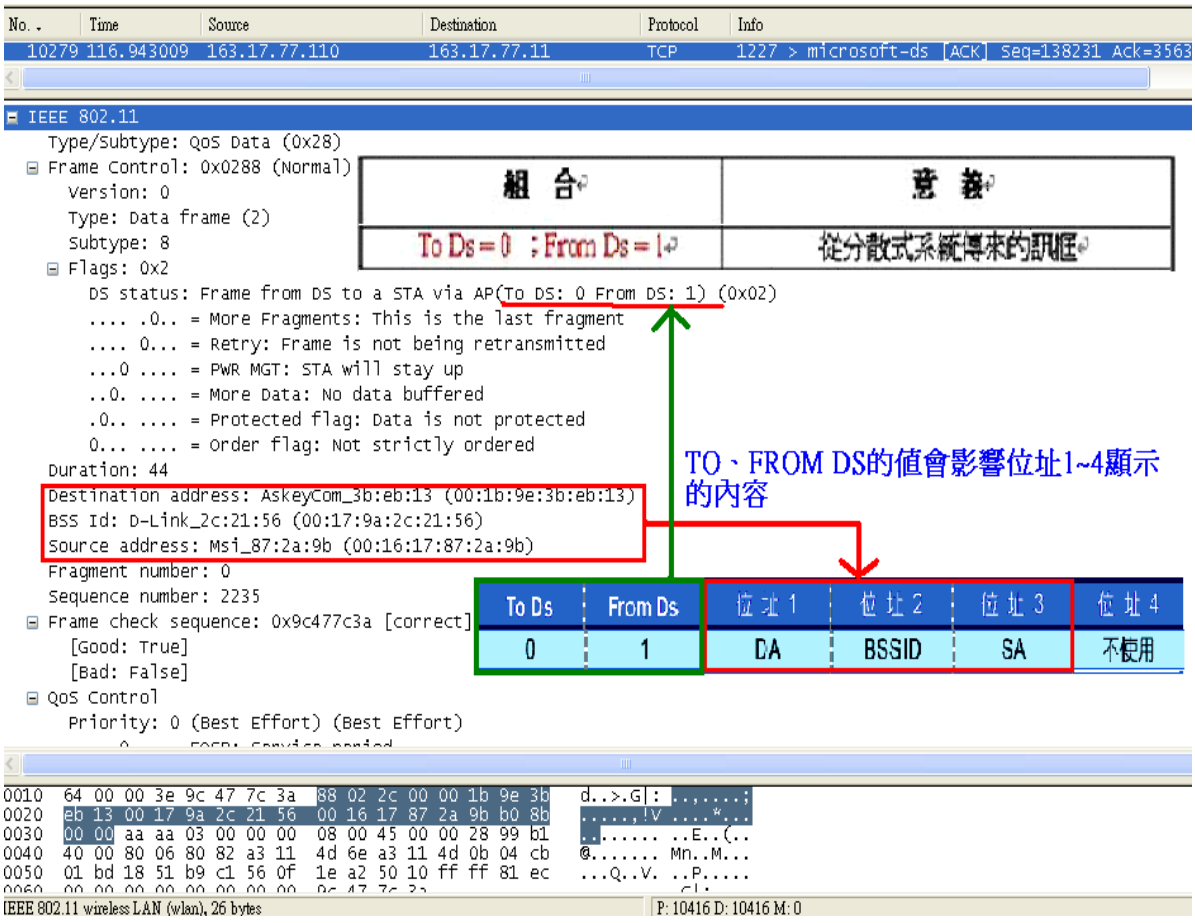


圖 4.5.3 封包資料 To DS =**0**／ From DS =**1** 訊框

(c) TO DS=1, FROM DS=1 時，代表是一個經分散式系統傳到另一個 BSS 內的主機。而位址 1~4 的內容分別為

位址 1：RA(接收端位址)

位址 2：TA(傳送端位址)

位址 3：DA(目的端位址)

位址 4：SA(來源端位址)

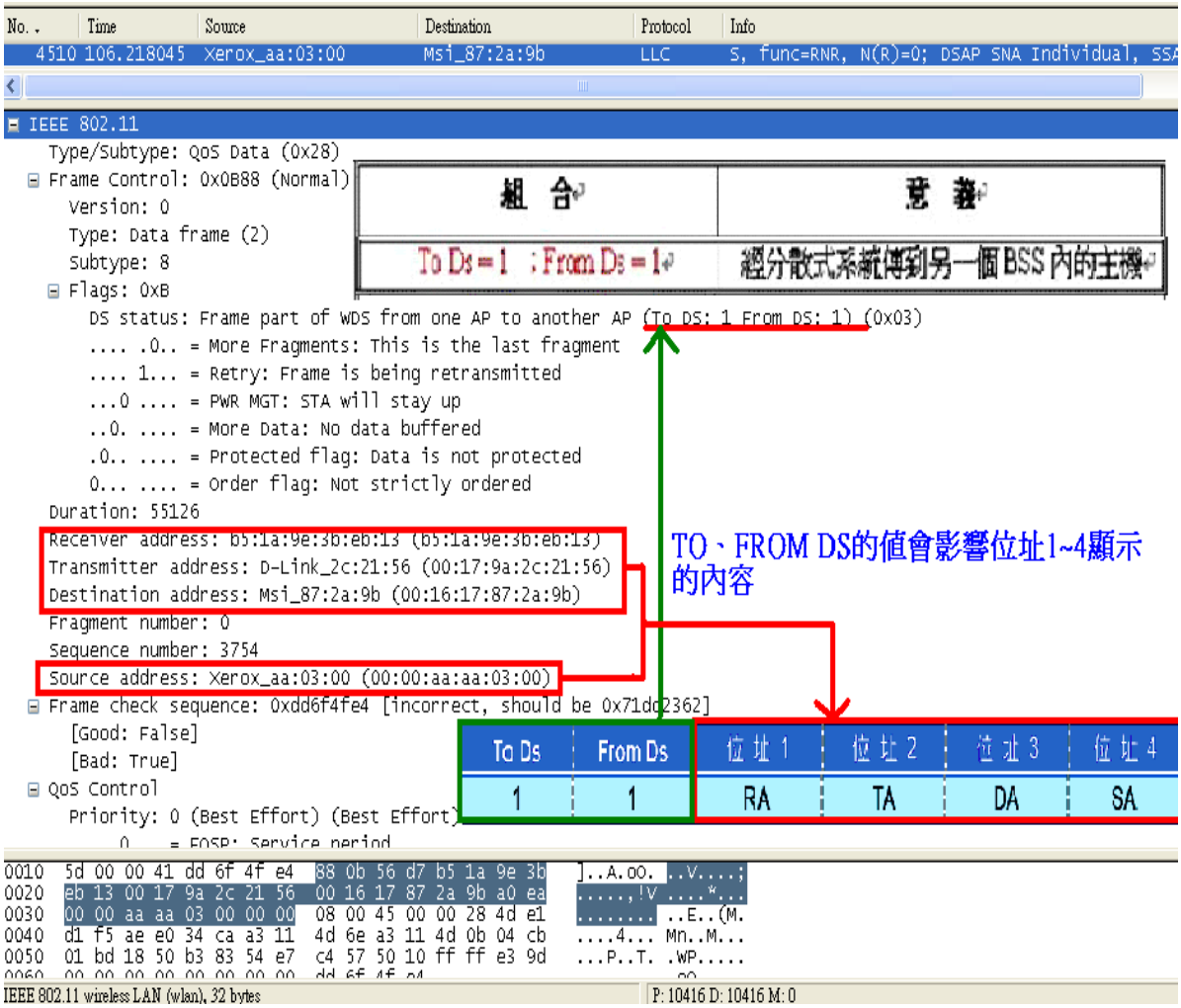


圖 4.5.4 封包資料 To DS =1／ From DS =1 訊框

(d) TO DS=0, FROM DS=0 時，代表是同一個 BSS，由一台主機傳給另一台主機。而位址 1~4 的內容分別為

位址 1：DA(目的端位址)

位址 2：SA(來源端位址)

位址 3：BSSID

位址 4：不使用

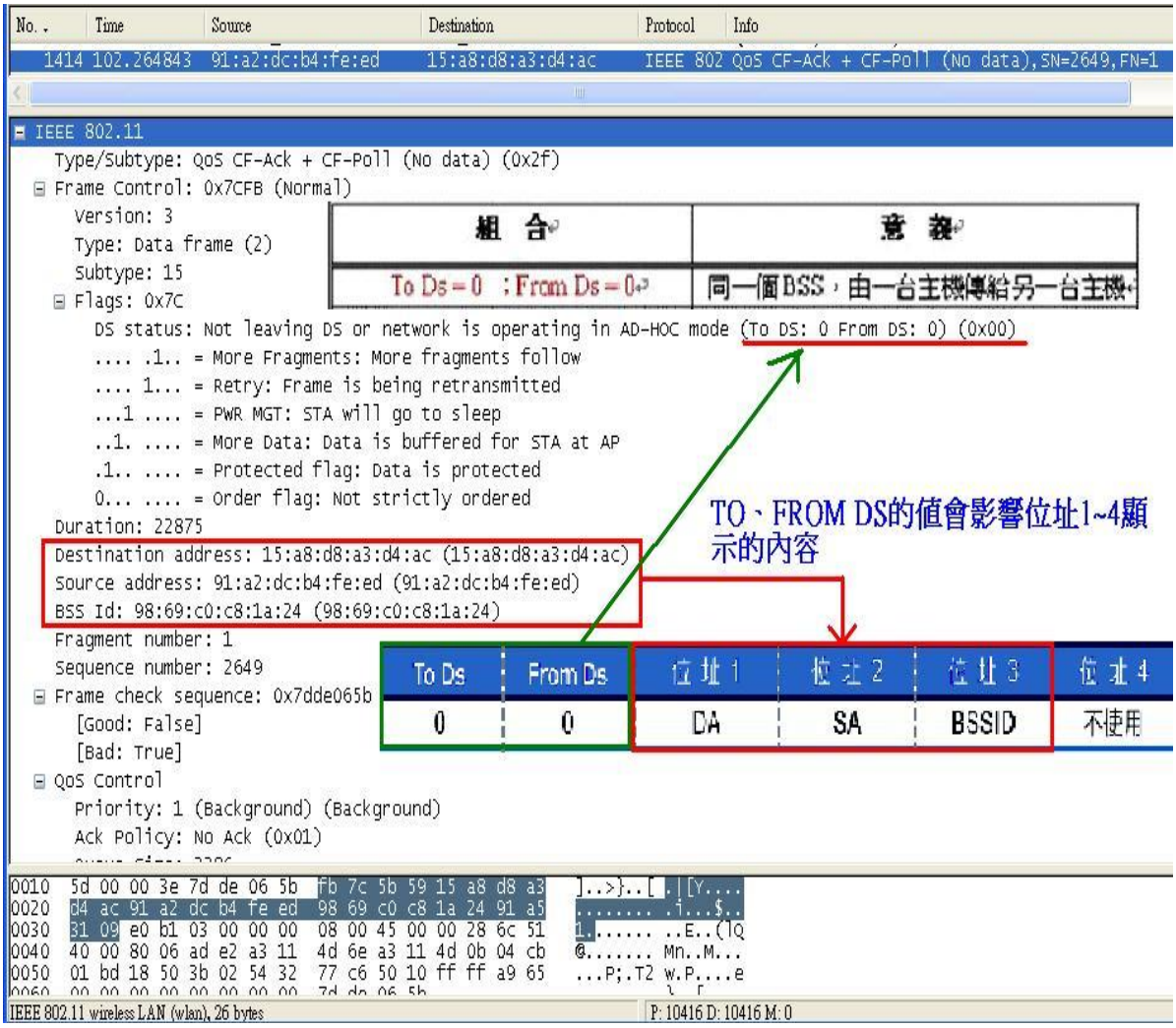


圖 4.5.5 封包資料 To DS =0／ From DS =0 訊框

4.6 Duration 封包介紹

在封包資料中點選 Duration (持續時間)資料查看，得到最下面的十六進制資料為 4c $8e_{(16)}$ ，為二進制的 0100 1100 1000 $1110_{(2)}$，但在換算前，由於封包擷取是從後面到前面，就類似資料結構的先進後出，因此以 8 位元方式前後將資料反過來為 1000 1110 0100 $1100_{(2)}$，經過換算後可知十進制為 36428 (= 32768 ＋ 2048 ＋ 1024 ＋ 512 ＋ 64 ＋ 8 ＋ 4)，對照 Duration 資料後可得到相同數值(如～圖中標示 1)。

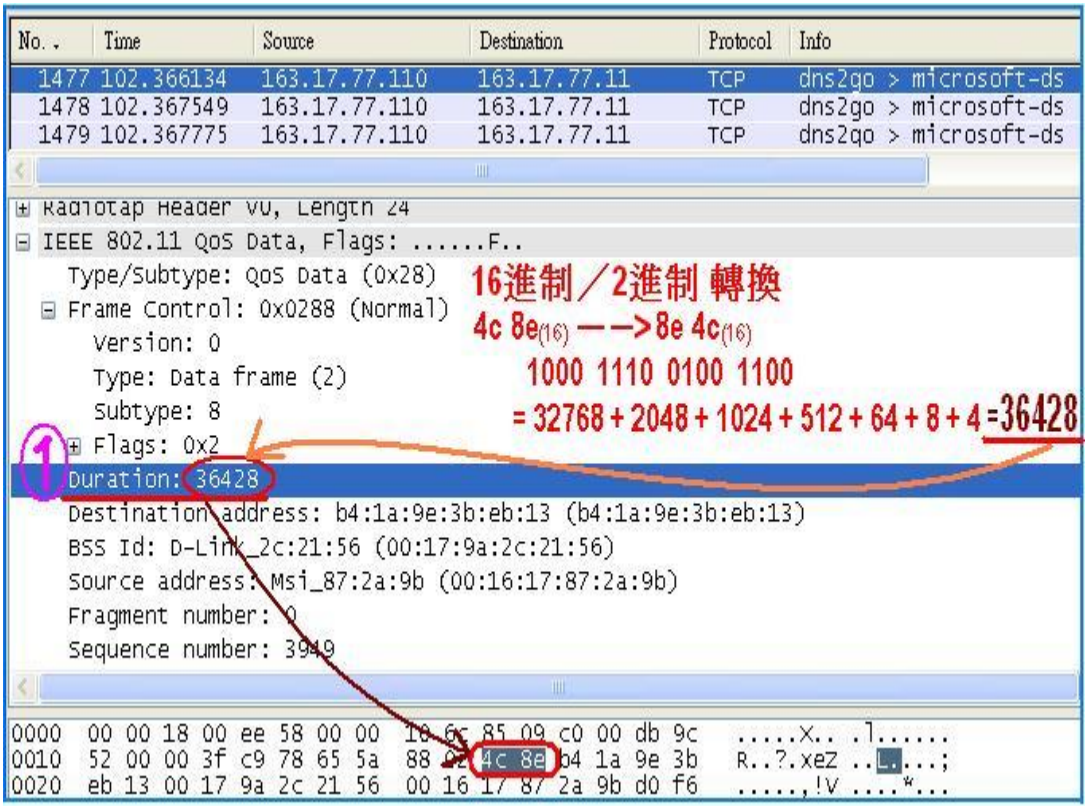


圖 4.6.1 封包資料 持續時間(Duration)訊框

Duration(持續時間)：依數值的不同有不同的用途，有些區塊暫時保留(Reserved)尚未定義，其他則主要提供傳送預計持續的時間或工作站 ID 使用。

表 1.7 Duration / ID 欄位中數值代表的時間

第15個位元	第14個位元	第13~0個位元	用途
0	0~32,767		持續時間
1	0	0	免競爭週期使用
1	0	1~16,383	保留
1	1	0	保留
1	1	1~2,007	記錄工作站的ID
1	1	2,008~16,383	保留

對照上表來看，由 4c8e(16 進制)轉成２進制的結果可知，第 15、14 個位元為 1 0(1000(2))，第 0～13 位元為 3660 的十進制，因此該欄位的用途沒有定義，為保留狀態。

另一個封包資料(如圖 4.6.2)

我們可以再看看另一筆封包資料，查看 To DS／From DS、Duration 的相關資訊，如下圖所示，在 Flags 資料的十六進制資料０１$_{(16)}$——＞0000 0001$_{(2)}$ (如～圖中標示 A2)　相反後——＞1000 0000，再對照中間資料後可得到相同的數值，To DS　＝１、From DS＝０(如～圖中標示 A1)。

＊ 其中 To DS：１／From DS：０所代表的意思是要傳送到分散式系統的訊框。

而 Duration 的資料為 2C 00$_{(16)}$ (如～圖中標示 B2)——＞0010 1100 0000 0000$_{(2)}$ 以 8 位元的方式前後將資料反過來後 0000 0000 0010 1100$_{(2)}$可得到十進制值 44(如～圖中標示 B1)。

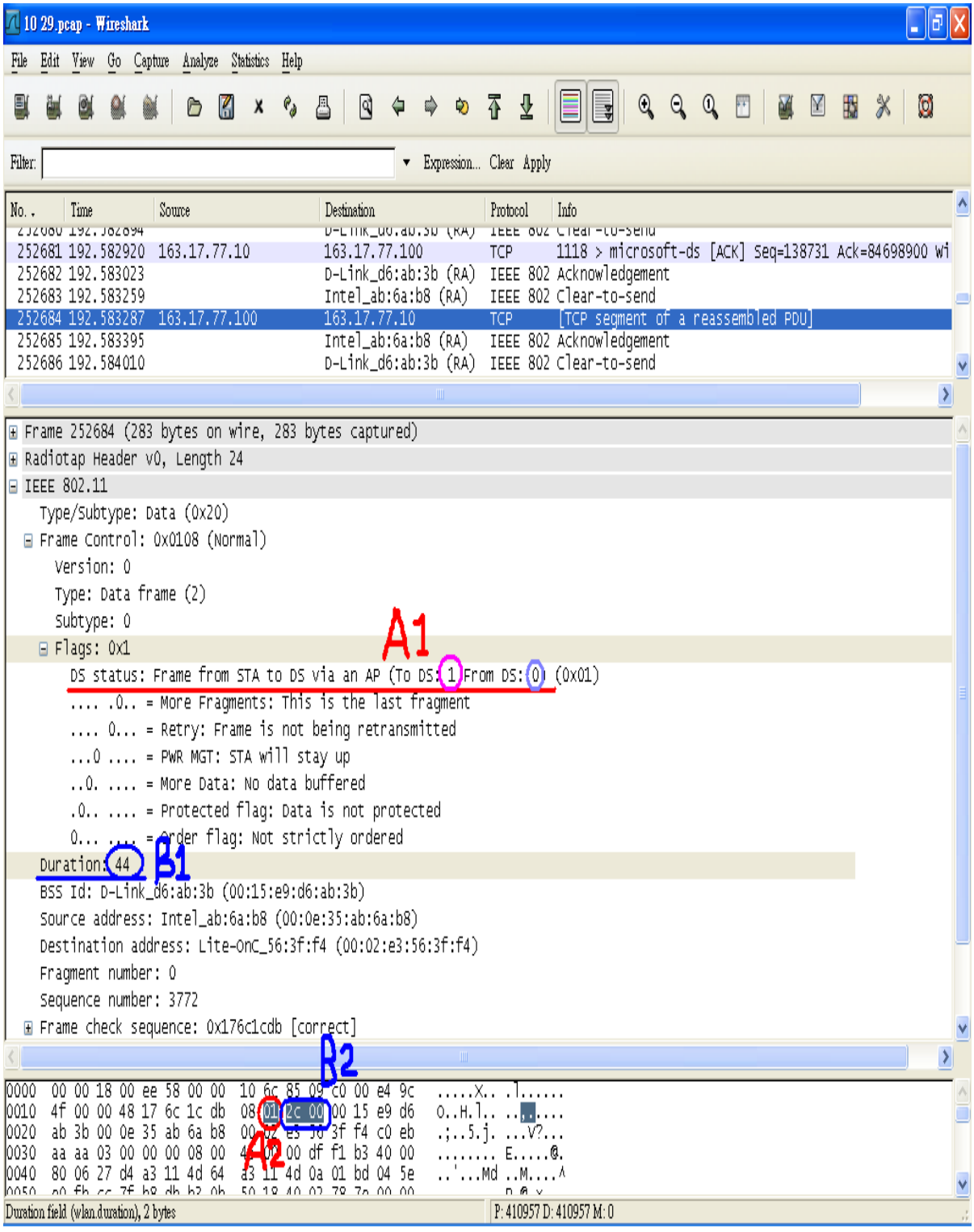


圖 4.6.2 To DS／From DS、持續時間(Duration)訊息

而通常 To DS 與 From DS 運用在一起，當 To DS ＝1 表示這訊框是要傳送到分散式系統，From DS ＝1 表示這訊框是從分散式系統傳來，前面的表 1.2 即為 To DS／From DS 在不同組合代表的意義。

第五章 錯誤案例

5.1 Ad Hoc 模式

1.先在兩台 NB 筆記型電腦 a、NB 筆記型電腦 b 開啟 TCP/IP 的內容，將 IP 位址設定成相同的網段（如～IP 位址：163.17.77.20 →NB 筆記型電腦 a、163.17.77.22 →NB 筆記型電腦 b），此時在筆記型電腦 a 設定一個 SSID=qwe 的名稱時(如圖 5.1.1 中標示 a)，筆記型電腦 b 在完全沒有任何 SSID 設定的情況下(如圖 5.1.2 中標示 a)，點選“檢視無線網路” 開啟時，按左方的重新整理網路清單，則會自行出現與筆記型電腦 a 相同的 SSID 名稱，並自動連線(如圖 5.1.3 所示)。

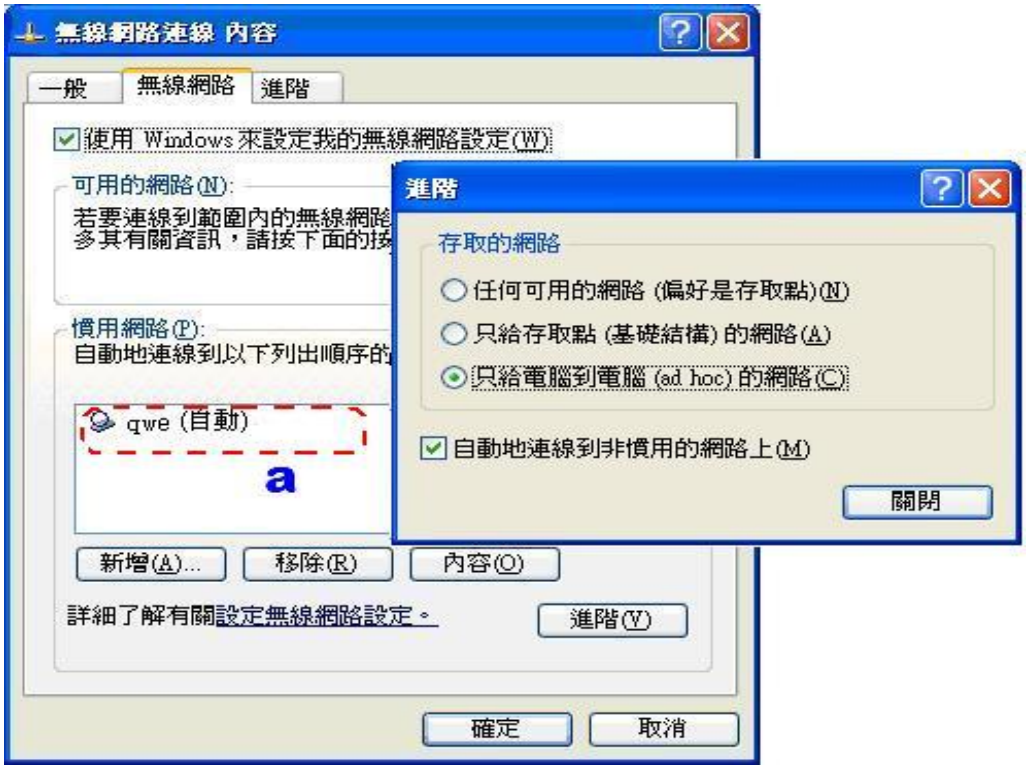


圖 5.1.1 錯誤案例 Ad Hoc SSID 設定-NB 筆記型電腦 a

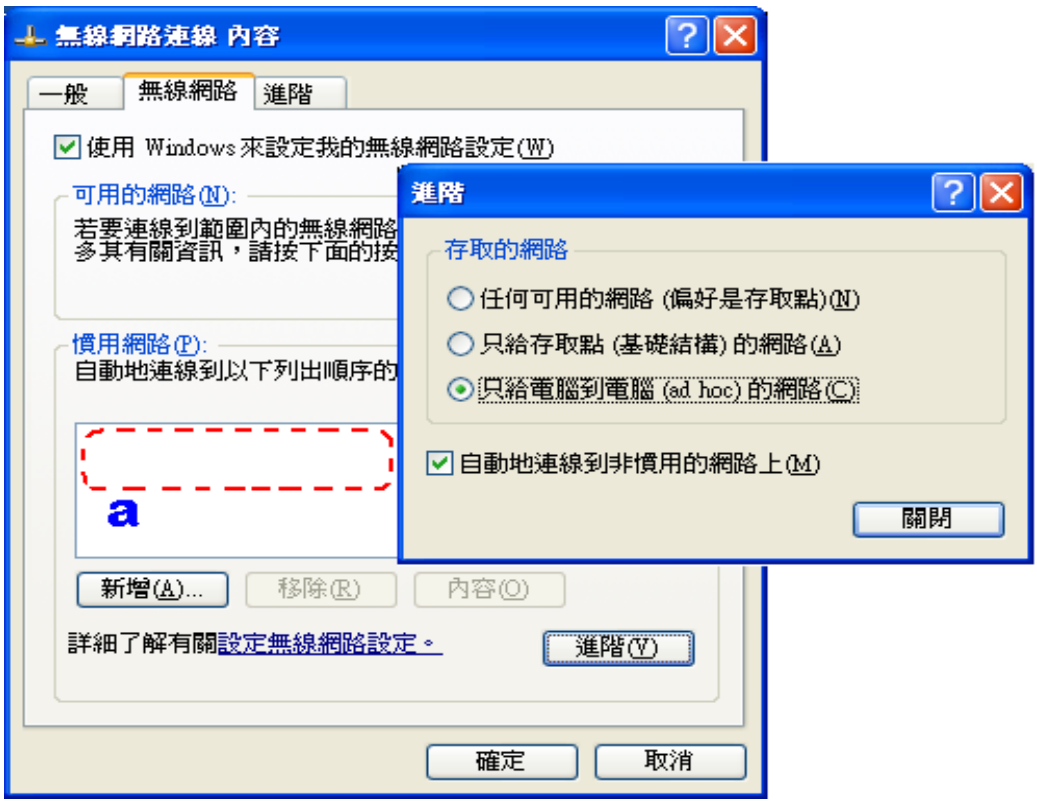


圖 5.1.2 錯誤案例 Ad Hoc SSID 設定-NB 筆記型電腦 b

圖 5.1.3 錯誤案例 Ad Hoc 「無線網路連線」視窗 -NB 筆記型電腦 b

5.2 Infrastructure 模式 - 透過單 1 台 AP

5.2.1 IEEE 802.11x 無線通訊協定–錯誤偵測比較

1.設定 PC 電腦／NB 筆記型電腦為同網段的私有 IP 位址後，將該環境的 PC 電腦慣用 DNS 伺服器設定在每台電腦內，接著開啟網頁進入 AP 的設定畫面，設定 SSID 和 AP 位址為 192.168.0.1 之後，在〝802.11g Only Mode〞欄位進行點選 Enabled 設定成只允許給 IEEE 802.11g 標準的電腦使用 (如圖 5.2.1)。

圖 5.2.1 錯誤案例 Infrastructure(802.11x 通訊協定) AP 設定 802.11**g** 標準

2.此時將控制台內「Windows 防火牆」的 ICMP 設定勾選後(如圖 5.2.2)，將 AirPcap 網卡插在 PC 電腦開啟 WireShark 封包軟體進行擷取封包。

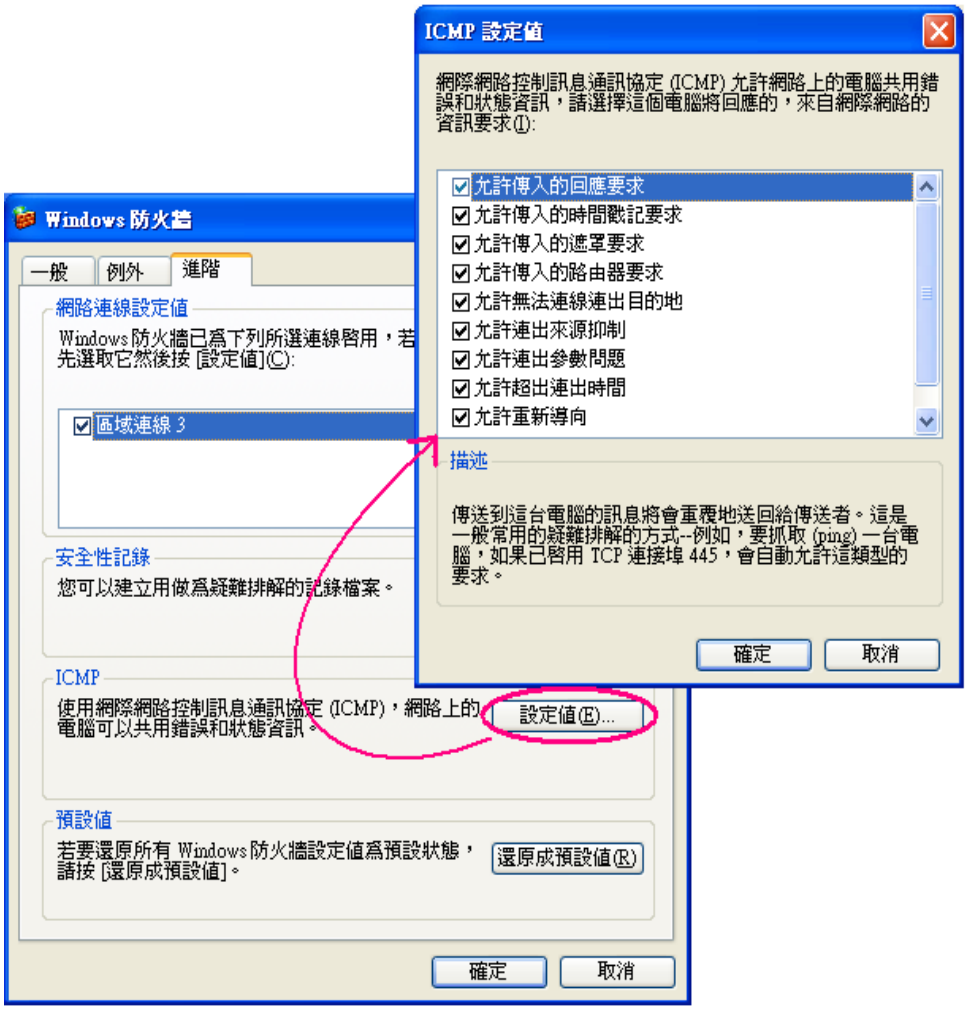


圖 5.2.2 錯誤案例 Infrastructure(802.11x 通訊協定) 防火牆設定 ICMP

3.接著運用 NB 筆記型電腦 a 透過 AP 進行連接時，都能夠順利存取到 PC 電腦中所分享的資料，並能透過 AP 連接到 LAN 端的有線網路，進而順利上網。但是運用 NB 筆記型電腦 b 進行連線存取資料時，卻無法透過 AP 順利的連接到網路。

此時在 NB 筆記型電腦 a 內點選無線網路連線內容，進行無線模式的查詢時，能得知電腦只支援 IEEE 802.11g 標準的通訊方式(如圖 5.2.3)，並且符合先前在 AP 網頁當中的〝802.11g Only Mode〞欄位設定，因此能順利連線。 接著在 NB 筆記型電腦 b 中進行無線模式的查詢時，能得知電腦只支援 IEEE 802.11b 標準，卻無法支援 IEEE 802.11g 的訊訊方式(如圖 5.2.4)，因此無法透過 AP 順利存取資料。

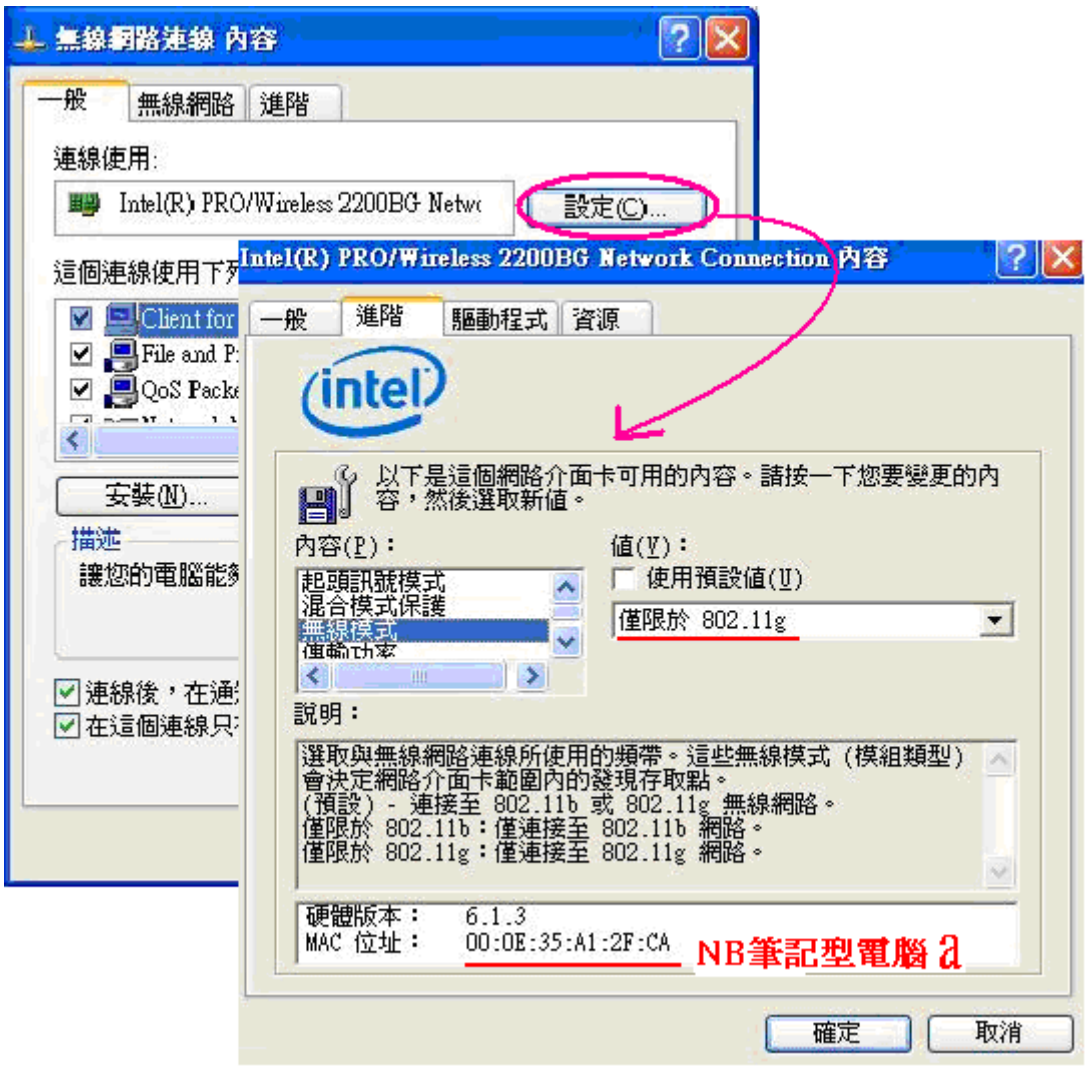


圖 5.2.3 錯誤案例 Infrastructure(802.11x 通訊協定) 無線模式 802.11x 查詢-NB 筆記型電腦 a

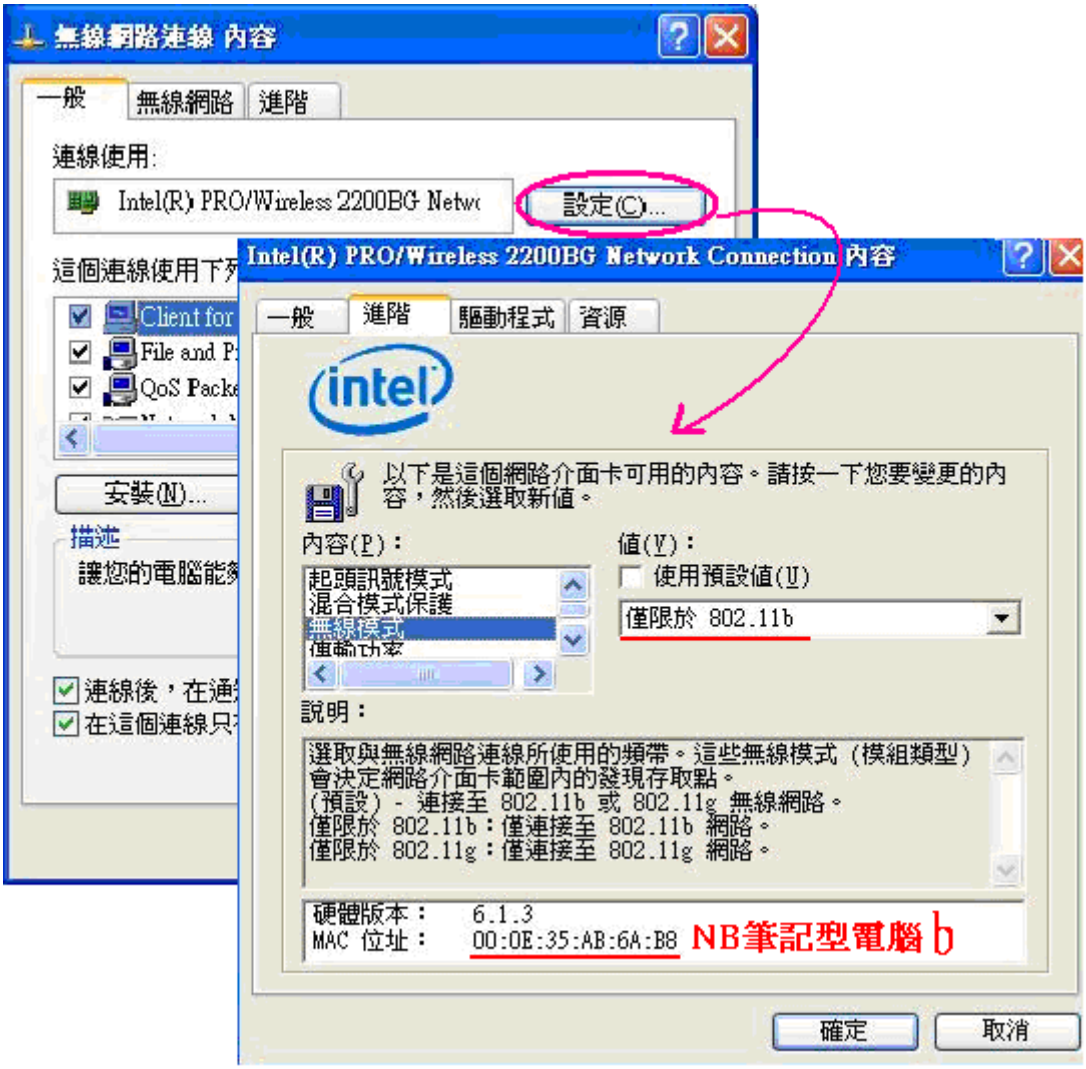


圖 5.2.4 錯誤案例 Infrastructure(802.11x 通訊協定) 無線模式 802.11x 查詢-NB 筆記型電腦 b

4.此時先查詢各台電腦的實體位址後，在擷取到的封包中進行 Filter 欄位的過濾設定，能看見 Source 來源端 NB 筆記型電腦 a(實體位址_00:0e:35:a1:2f: ca)透過 Destination 目的端的 AP(實體位址_00:17:9a:2c:21:56)連線時，雙方都能得到呼叫及回應的結果，進而順利連線(如圖 5.2.5)。

接著在過濾欄位點選 Clear 取消過濾後，在 Filter 欄位輸入 NB 筆記型電腦 b 的過濾指令後，可得知由於 AP 只支援 IEEE 802.11g 的通訊協定，造成 NB 筆記型電腦 b 所擁有的 IEEE 802.11b 通訊協定，無法透過 AP 連到 PC 電腦(如圖 5.2.6)，也因此無法順利連到外面的網際網路。

Filter 欄位指令
(arp && wlan.addr==00:0e:35:ab:6a:b8) || wlan.addr==00:0e:35:a1:2f:ca

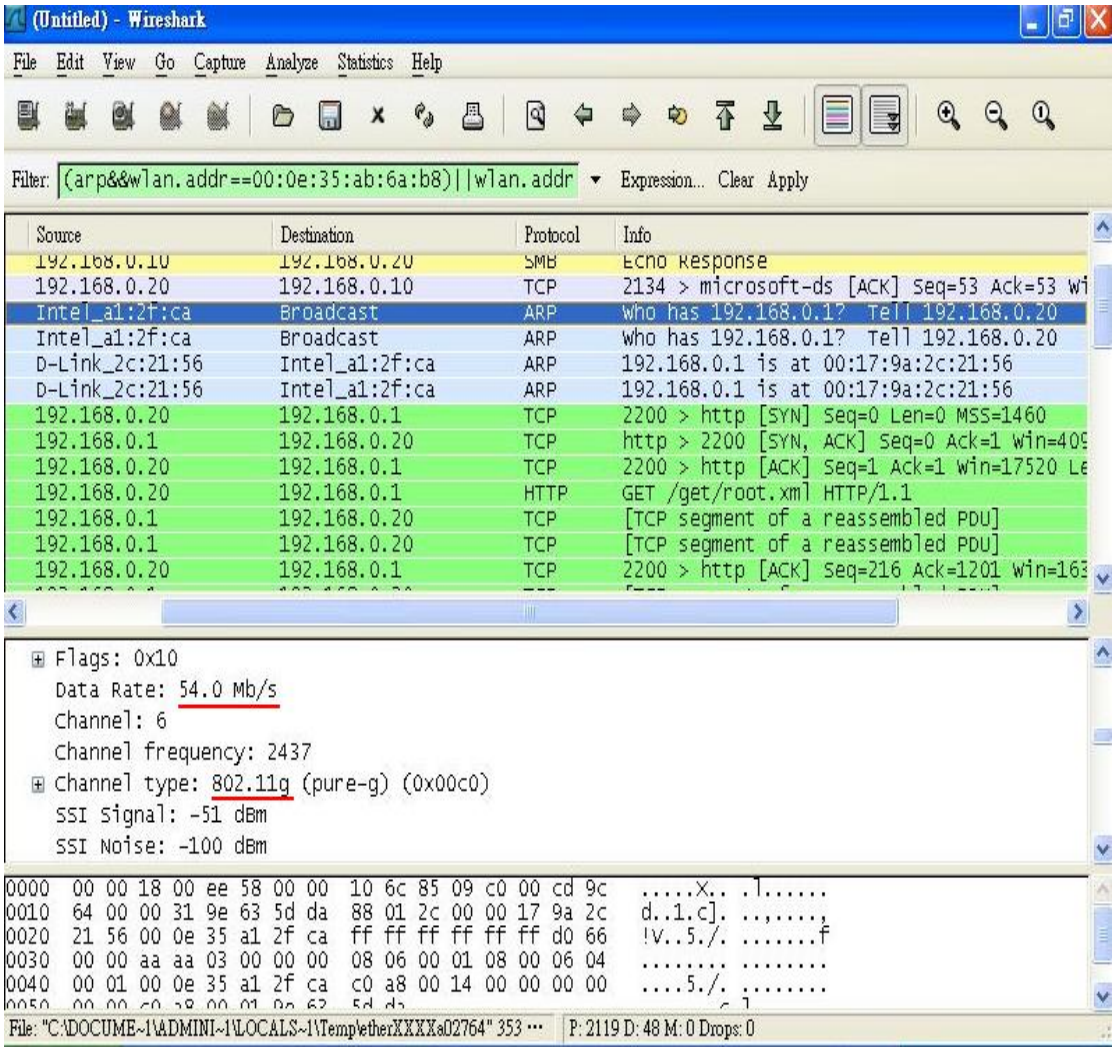


圖 5.2.5 錯誤案例 Infrastructure(802.11x 通訊協定) 封包-NB 筆記型電腦 a 順利連到網路

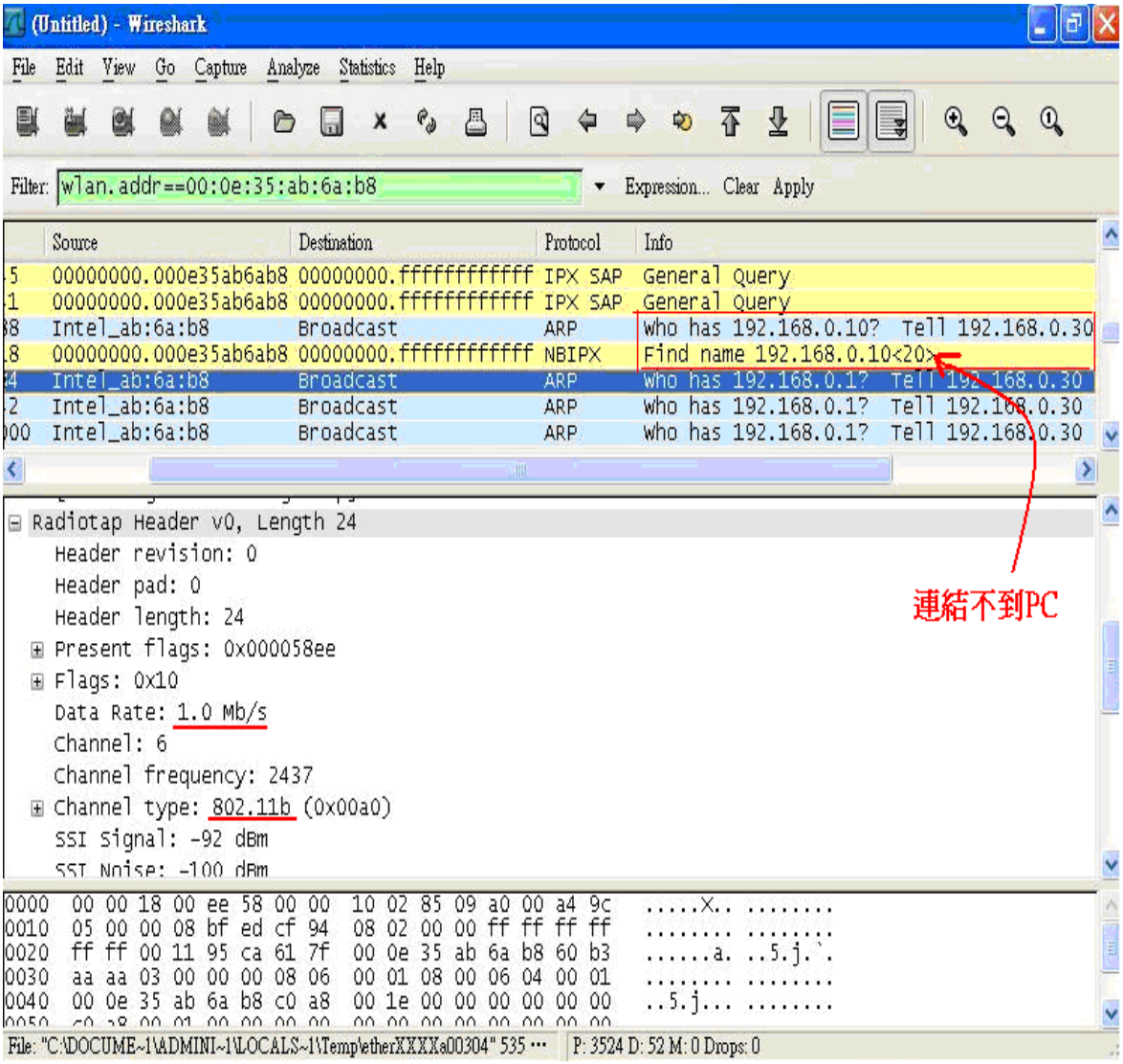


圖 5.2.6 錯誤案例 Infrastructure(802.11x 通訊協定) 封包-NB 筆記型電腦 b 無法連結 PC 電腦

5.接著在 AP 的設定網頁中將〝802.11g Only Mode〞欄位點選為 Disabled，以設定成讓 IEEE 802.11b 與 IEEE 802.11g 通訊協定的電腦都能使用(如圖 5.2.7)。

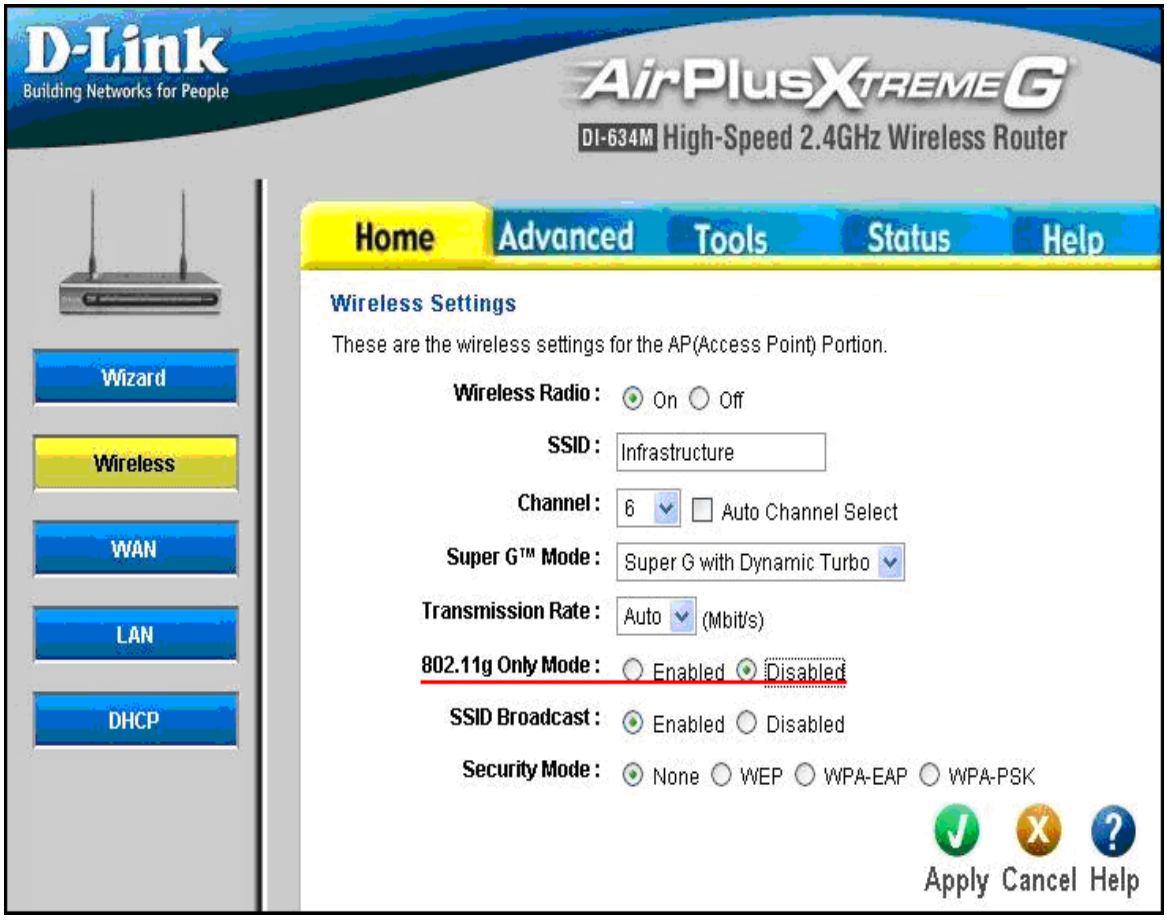


圖 5.2.7 錯誤案例 Infrastructure(802.11x 通訊協定) AP 設定 802.11**b/g** 標準

6.此時使用擷取到的封包資料進行 Filter 欄位的過濾時，可知 Source 來源端的 NB 筆記型電腦 a(實體位址_00:0e:35:a1:2f:ca)呼叫 Destination 目的端的 AP 進行連線時，能得到 AP 的回應(如圖 5.2.8 標示 a)；且來源端的 NB 筆記型電腦 b(實體位址_00:0e:35:ab:6a:b8)呼叫目的端的 AP 進行連線時，也能得到 AP 的回應(如圖 5.2.8 標示 b)。因此 NB 筆記型電腦 a、NB 筆記型電腦 b 都能透過 AP 順利傳資料給 PC 電腦，進而順利的上網。

Filter 欄位指令
(arp && wlan.addr eq 00:0e:35:a1:2f:ca)||(arp && wlan.addr eq 00:0e:35:ab:6a:b8)

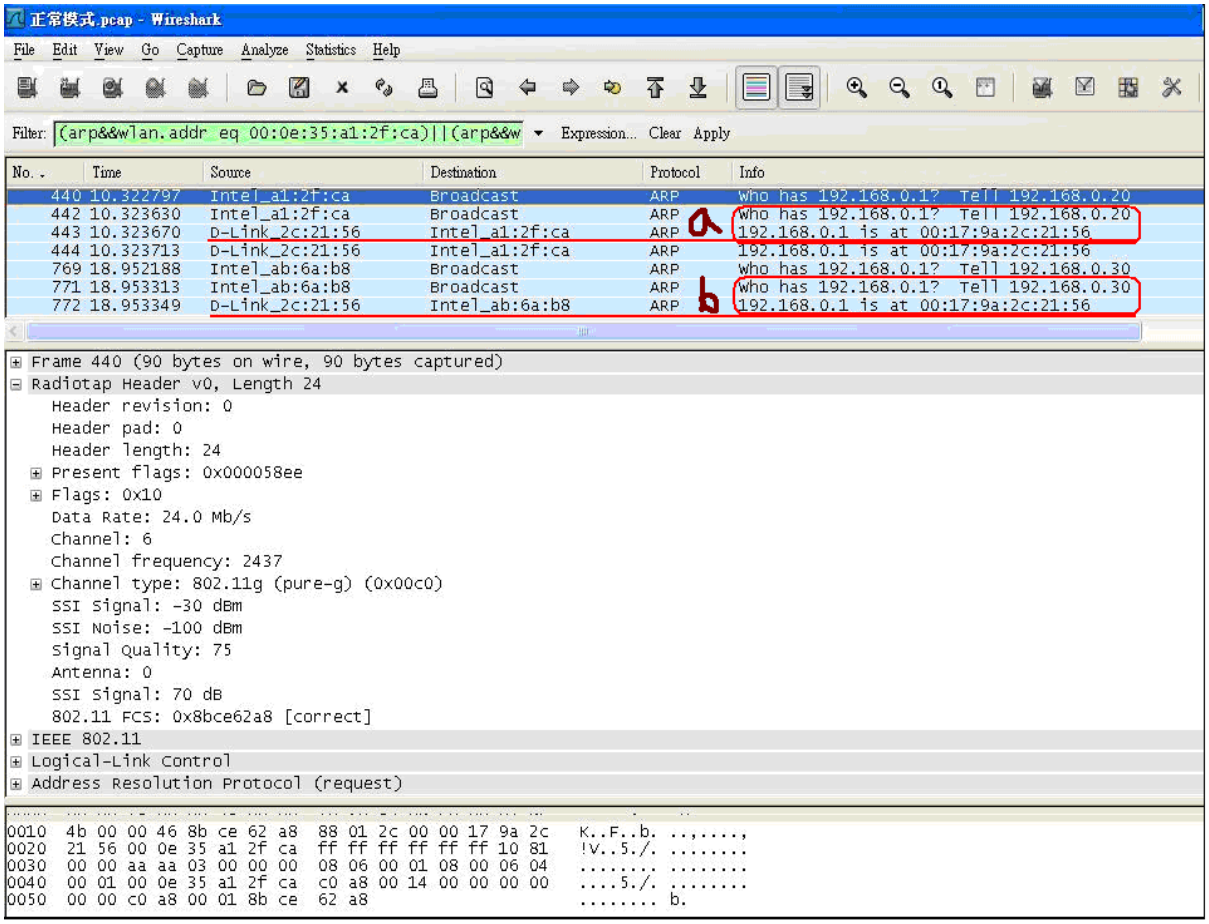


圖 5.2.8 錯誤案例 Infrastructure(802.11x 通訊協定) 封包-NB 筆記型電腦透過 AP 順利連結

7.如下圖封包所示，IEEE 802.11g 的 NB 筆記型電腦 a 跟 PC 電腦互相傳送資料時，顯示出當時以速率 48 Mb/s 進行傳送；而 IEEE 802.11b 的 NB 筆記型電腦 b 則是以 11Mb/s 的傳輸速率，跟 PC 電腦進行資料的傳送(如圖 5.2.9)。

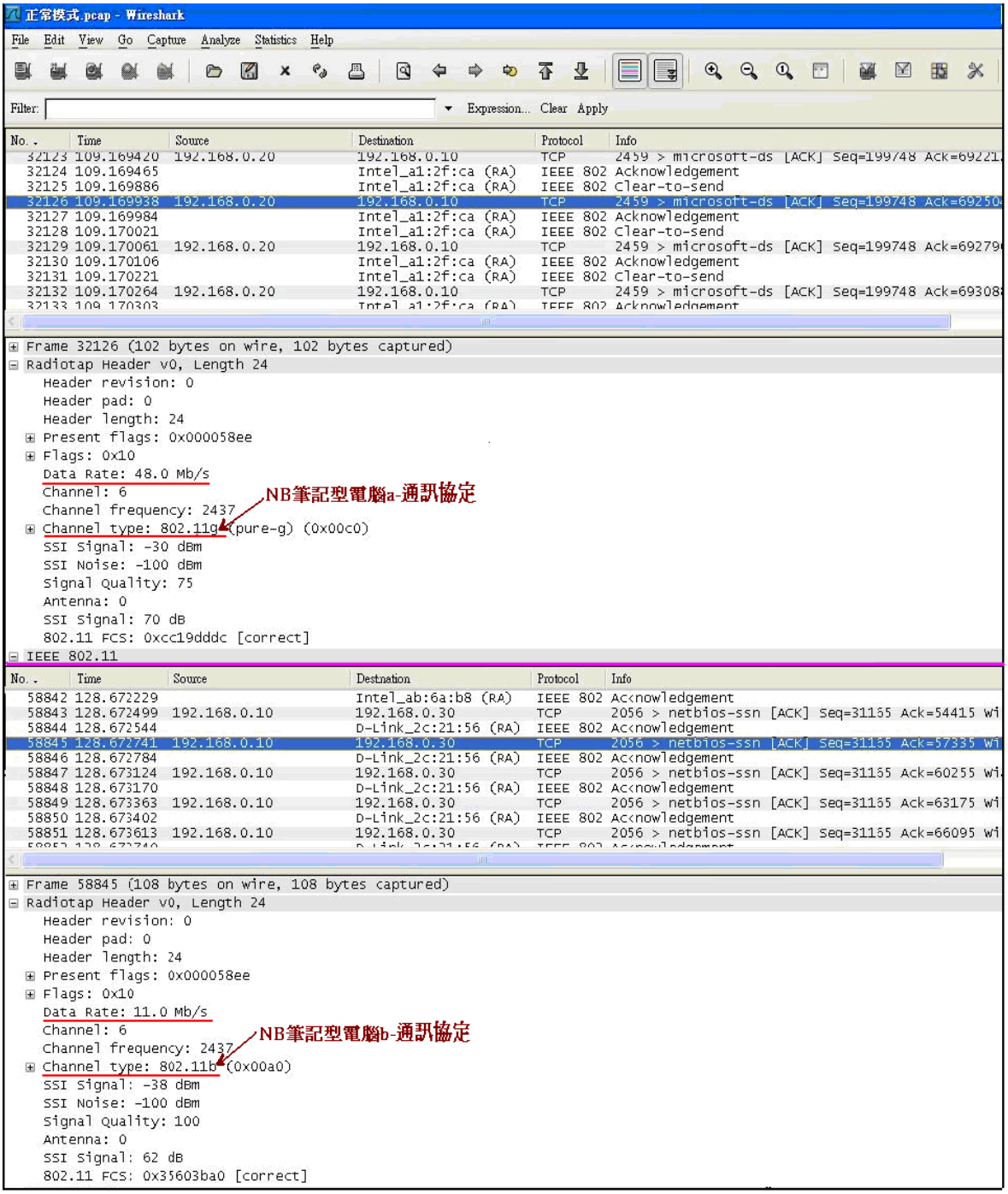


圖 5.2.9 錯誤案例 Infrastructure(802.11x 通訊協定) 封包-NB 筆記型電腦的傳輸速率

5.2.2 AP 設定金鑰模式加密

1.設定 PC 電腦／NB 筆記型電腦為同網段的私有 IP 位址後，將該環境的 PC 電腦慣用 DNS 伺服器設定在每台電腦內，接著開啟網頁進入 AP 的設定畫面，設定 SSID 和 AP 位址為 192.168.0.1 之後，選 WEP 進行金鑰模式的加密。

2.而 AP 和無線網路裝置之間要做連線時，都必順先經過一段協調過程，所以要在 WEP 畫面中進行設定(如圖 5.2.10)，這個步驟完成後要求進行認證程序，而這項設定分別有兩種方式，第一種是 Open System Aauthentication，另一種為 Shared Key Authentication。使用預設的 Open System 時，在不提供任何安全機制下，任何使用者都能透過 AP 連線到網路並進行存取，但在這種情況下並沒有任何的保障。 反之，如果點選 Shared Key 時，AP 和使用者之間就會進行一段認證過程，此時就能讓無線網路有高安全性的環境。

所以在設定 AP 金鑰模式進行加密時，為了有更好的安全性，我們點選 Shared Key 後，在 WEP Key1 的欄位內進行密碼的設定

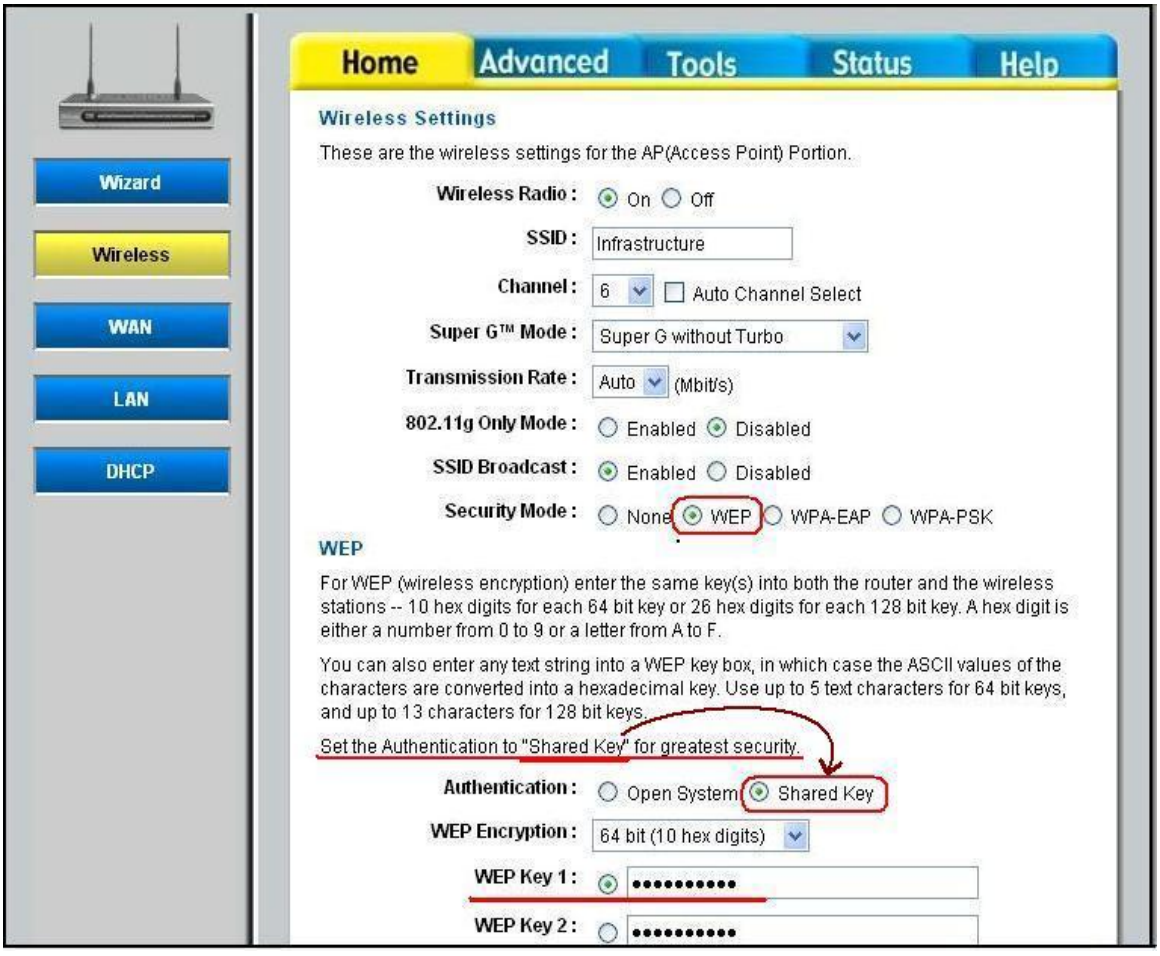


圖 5.2.10 錯誤案例 Infrastructure(金鑰加密) AP 網頁的密碼設定

3.接著將控制台內「Windows 防火牆」的 ICMP 設定勾選後(如前面的圖 5.2.2)，將 AirPcap 網卡插在 PC 電腦開啟 WireShark 封包軟體進行擷取封包。此時在 NB 筆記型電腦 a 開啟無線網路連線視窗，點選 Infrastructure(SSID)進行連線時，就會要求使用者輸入金鑰密碼(如圖 5.2.11)，並透過 AP 連線到該無線網路的環境。

圖 5.2.11 錯誤案例 Infrastructure(金鑰加密) 筆記型電腦 b 連結 AP 的金鑰設定

5.輸入好正確的金鑰密碼後進行連結測試時，等待一段時間卻一直無法跟 AP 順利連線(如圖 5.2.12)。

圖 5.2.12 錯誤案例 Infrastructure(金鑰加密) 筆記型電腦 b 連結 AP 的連線測試

6.此時先查詢各台電腦的實體位址後，在擷取到的封包資料的 Source 來源端與 Destination 目的端的欄位中，尋找與各台電腦相浮合的實體位址進行查詢。在下面的封包畫面當中，顯示來源端的 NB 筆記型電腦 a 呼叫目的端的 D-Link AP 要跟它連線時，都能夠順利呼叫並給予 Successful 的回應(如圖 5.2.13)，但由於 NB 筆記型電腦 a 不支援先前設定的 Shared Key 模式，使得 NB 筆記型電腦 a 一直無法跟 AP 順利連線(如圖 5.2.14)。

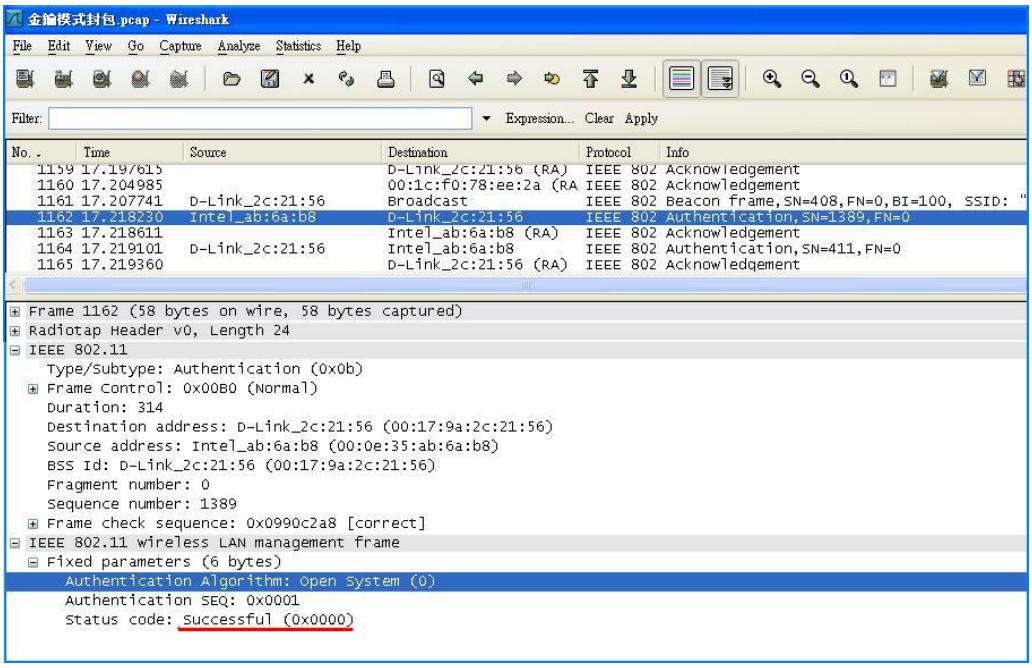


圖 5.2.13 錯誤案例 Infrastructure(金鑰加密) 筆記型電腦 b 呼叫 AP 的封包訊息

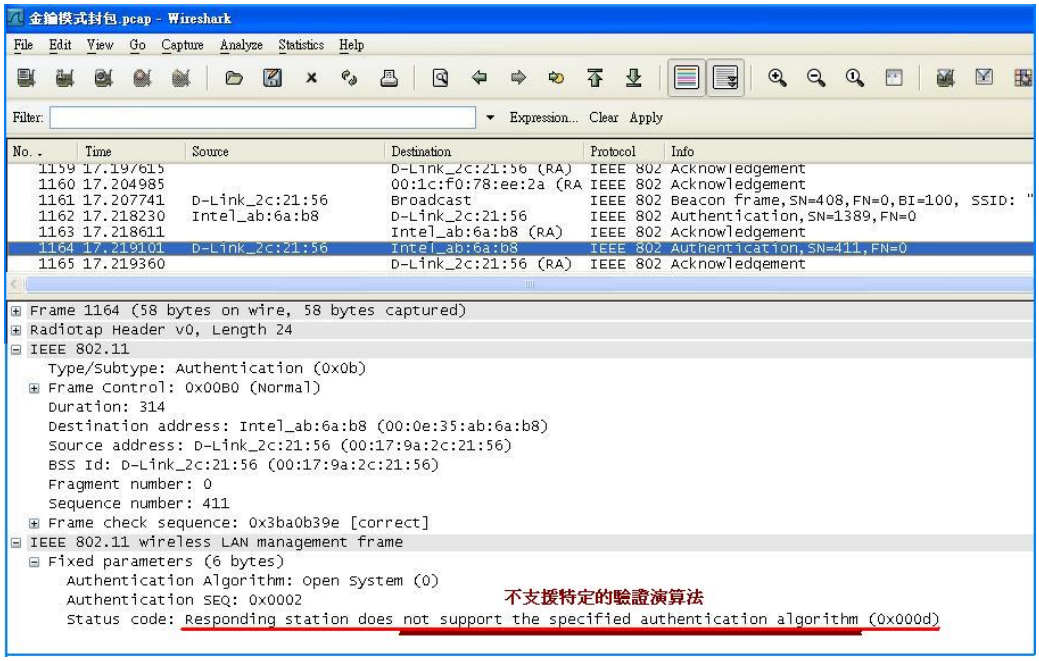
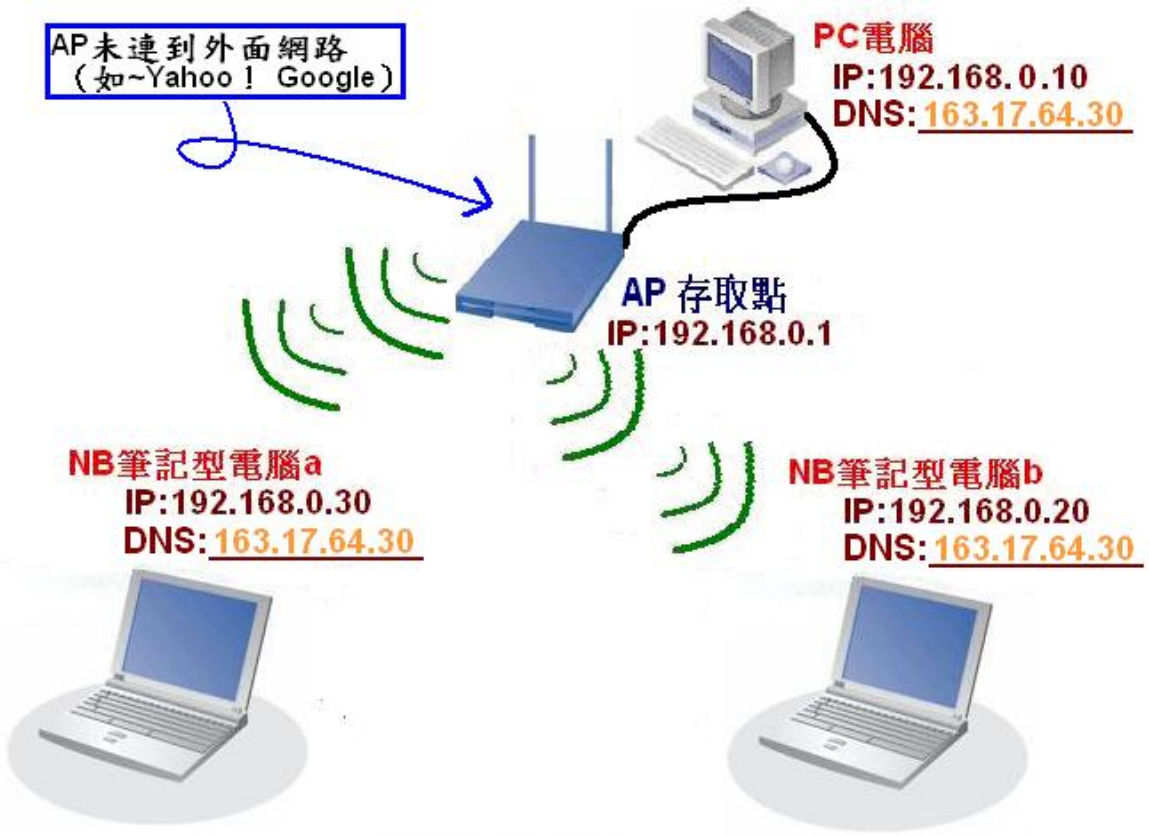


圖 5.2.14 錯誤案例 Infrastructure(金鑰加密) AP 回應筆記型電腦 b 的封包訊息

5.2.3 AP 未連到外面網路

1.設定 PC 電腦／NB 筆記型電腦為私有 IP 位址(同網段)，並以 AP 位址設為預設閘道後，將該環境的 PC 電腦慣用 DNS 伺服器設定在每台電腦內，接著開啟網頁進入 AP 的設定畫面，設定 SSID 和 AP 位址為 192.168.0.1 完成後，此時 AP 無法跟外面的網際網路連線(或許是連到到外 LAN 端的網路線沒接好，或者網路線在硬體方的失真斷線)。



2.接著將控制台內「Windows 防火牆」的 ICMP 設定勾選後(如前面圖 5.2.2)，將 AirPcap 網卡插在 PC 電腦開始擷取封包，此時在 NB 筆記型電腦 b 的執行視窗以 cmd 開啟命令提示畫面，一開始以指令 ping 做互連的動作時，每台電腦都可以跟對方順利連線，然面再試著以指令 ping 到知名網站時(如 Yahoo！ Google 網址)，卻出現連線失敗的結果(如圖 5.2.15)，因此無法順利上網。

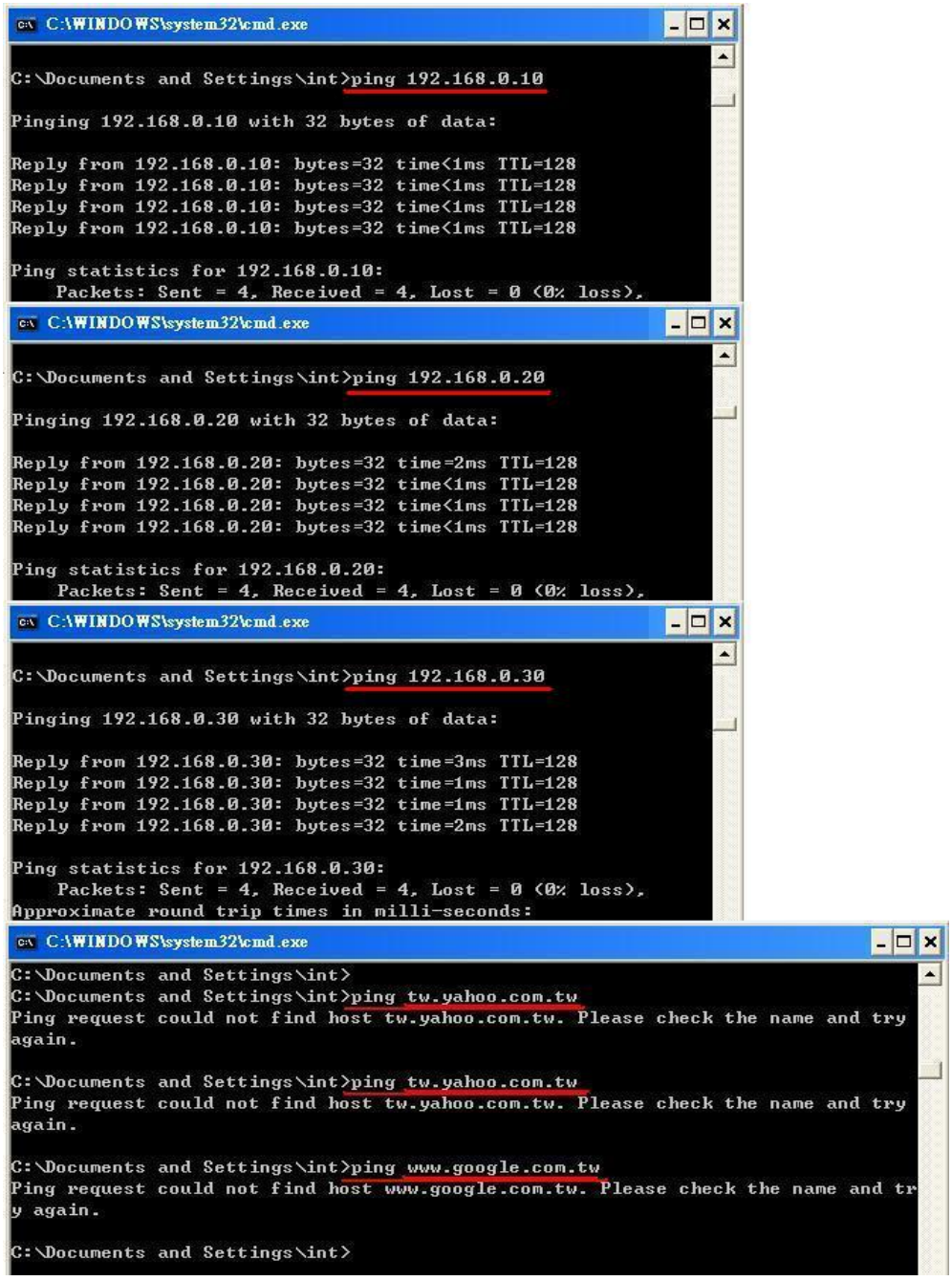


圖 5.2.15 錯誤案例 Infrastructure(AP 未連到外) 命令提示視窗- NB 筆記型電腦 b

3.此時將擷取到的封包，在 Filter 欄位以指令 arp || icmp || dns 過濾時可知，一開始用同一個網段的電腦互相連線時，能順利互通，例如 Source 來源端的筆記型電腦 b，能夠與 Destination 目的端的筆記型電腦 a 互相連線，而無法連到外面的網際網路(如圖 5.2.16)。由此可知，因為另一邊的 LAN 端路由器的錯誤，使我們與網路隔絕，而無法上網，因此這並不是區域網路設定或設備上的問題，且另一邊的設定我們也無法做修正。

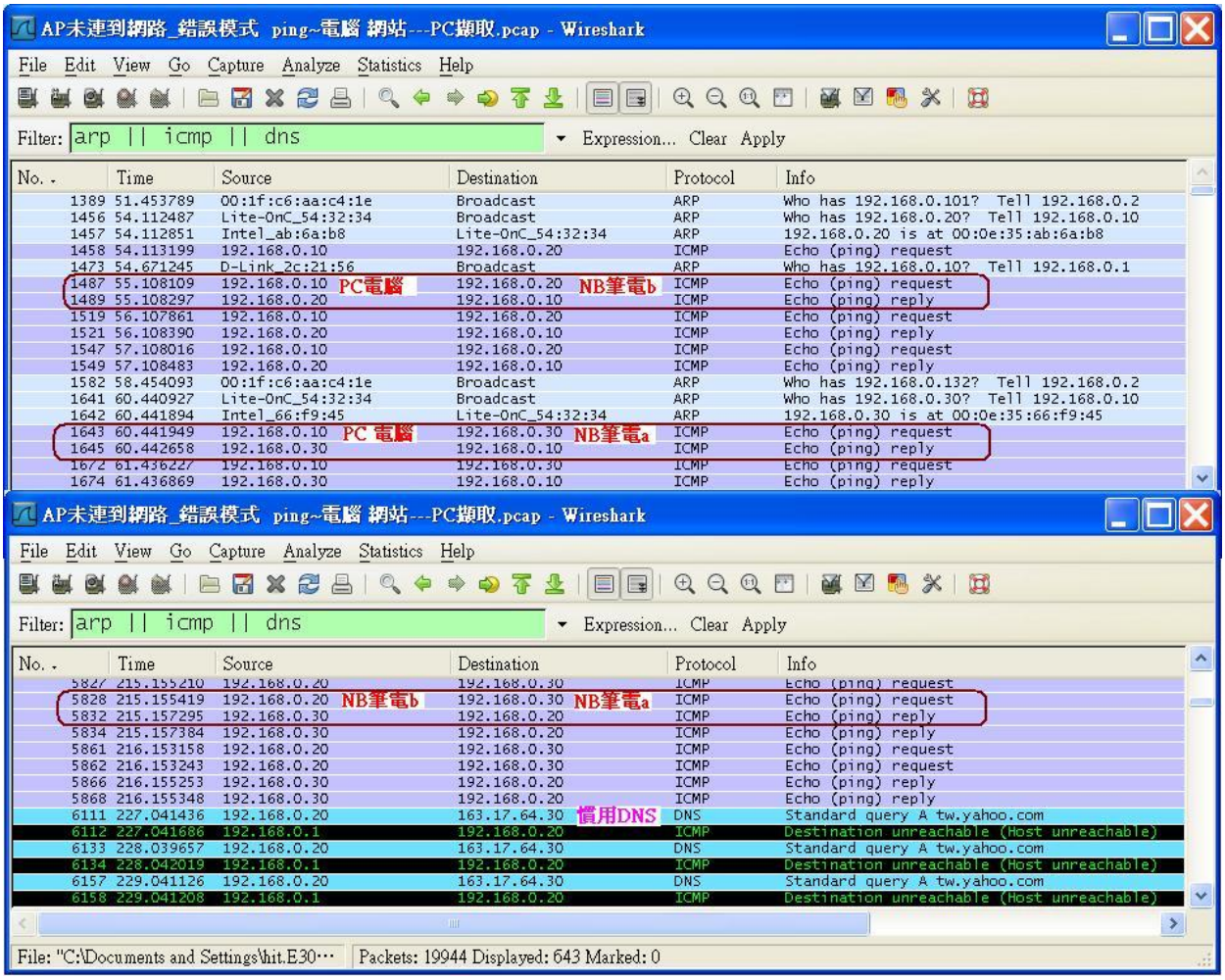


圖 5.2.16 錯誤案例 Infrastructure(AP 未連到外) 封包擷取結果

參 考 文 獻

書籍

1. 網路概論與實務 第二版 楊豐瑞/楊豐任 編著

網站

[1] http://www.cs.nthu.edu.tw/~nfhuang/chap13.htm#13.4 IEEE 802.11 Wireless LAN 網路

[2] http://vfhhu.pixnet.net/blog/post/17600066 無心呢喃

[3] http://www.netadmin.com.tw/article_content.asp?sn=0808050013

[4] http://blog.shaolin.tw/2008/03/wireshark.html 少・林: Wireshark 教學

[5] http://blog.chinaunix.net/u2/72886/article_97513.html

[6] http://life.iiietc.ncu.edu.tw/xms/content/show.php?id=17810

[7] http://www.usc.edu.tw/cc/wireless/word.htm